

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-29966  
(P2000-29966A)

(43) 公開日 平成12年1月28日 (2000.1.28)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	サーチコード (参考)
G 0 6 F 19/00		G 0 6 F 15/30	3 5 0 A 3 E 0 4 0
G 0 7 F 19/00			M 5 B 0 5 5
			3 1 0
		G 0 7 D 9/00	4 7 6

審査請求 未請求 請求項の数13 O L (全 36 頁)

(21) 出願番号 特願平10-196109

(22) 出願日 平成10年7月10日 (1998.7.10)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72) 発明者 三石 和幸

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(72) 発明者 岸野 琢己

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(74) 代理人 100089118

弁理士 酒井 宏明

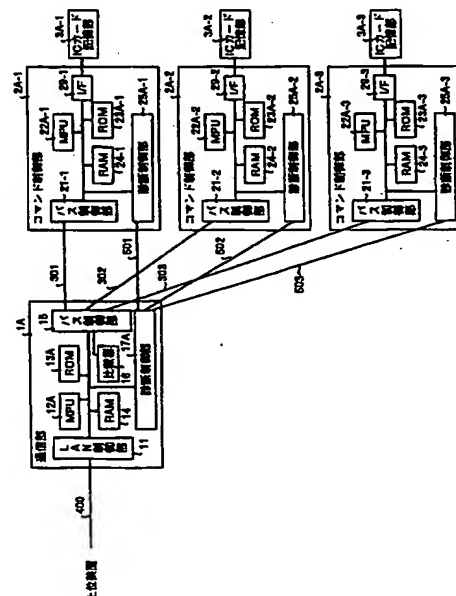
最終頁に続く

(54) 【発明の名称】 電子現金用金庫および電子マネーシステム

(57) 【要約】 (修正有)

【課題】 多重化制御による価値の多重引き出しを防止することを課題とする。

【解決手段】 バスインタフェース301~303で、通信部1A側から各コマンド制御部2A-1~2A-3側へ上位装置からのコマンドを転送するとともにそのコマンド処理結果を各コマンド制御部2A-1~2A-3側から通信部1A側へ転送し、診断チェックパス501~503で、通信部1A側から各コマンド制御部2A-1~2A-3側へ診断のためのコマンドを転送するとともにその診断結果を各コマンド制御部2A-1~2A-3側から通信部1A側へ転送する。診断結果で正常と判定されたコマンド制御部に対して上位装置から受け取ったコマンドを転送してコマンド処理を実行する。



BEST AVAILABLE COPY

## 【特許請求の範囲】

【請求項1】 通貨の価値を電子的な情報で表した電子現金を記憶する複数の記憶部を有し、利用者とのICカードとの間で電子現金の移転を行うための電子現金用金庫であって、

前記複数の記憶部に対するコマンドを並列的に実行し、前記複数の記憶部の制御機能を実現する複数のコマンド制御部と、

前記複数のコマンド制御部との間にコマンド数に相当する通信バスを並列的に形成し、前記複数の記憶部との通信機能を実現する通信部と、

前記複数のコマンド制御部と前記通信部とを接続し、前記通信部の制御に従って、通信部側からコマンド制御部側へ電子現金移転のためのコマンドを転送するとともにそのコマンド処理結果をコマンド制御部側から通信部側へ転送する第1インタフェース手段と、

前記複数のコマンド制御部と前記通信部とを接続し、前記通信部の制御に従って、通信部側からコマンド制御部側へ診断のためのコマンドを転送するとともにその診断結果をコマンド制御部側から通信部側へ転送する第2インタフェース手段と、

を備えたことを特徴とする電子現金用金庫。

【請求項2】 前記通信部は、前記第2インタフェース手段による診断処理を前記第1インタフェース手段によるコマンド処理とは独立して制御し、前記各コマンド制御部は、前記第2インタフェース手段による診断処理を前記第1インタフェース手段によるコマンド処理とは独立して実行することを特徴とする請求項1に記載の電子現金用金庫。

【請求項3】 通貨の価値を電子的な情報で表した電子現金を記憶する複数の記憶部を有し、利用者とのICカードとの間で電子現金の移転を行うための電子現金用金庫であって、

前記複数の記憶部に対するコマンドを並列的に実行し、前記複数の記憶部の制御機能を実現する複数のコマンド制御部と、

前記複数のコマンド制御部との間にコマンド数に相当する通信バスを並列的に形成し、前記複数の記憶部との通信機能を実現する通信部と、

前記複数のコマンド制御部と前記通信部とを接続し、前記通信部の制御に従って、通信部側からコマンド制御部側へ電子現金移転のためのコマンドを転送するとともにそのコマンド処理結果をコマンド制御部側から通信部側へ転送することに加え、通信部側からコマンド制御部側へ診断のためのコマンドを転送するとともにその診断結果をコマンド制御部側から通信部側へ転送するインタフェース手段と、

を備えたことを特徴とする電子現金用金庫。

【請求項4】 前記通信部は、前記複数のコマンド制御部に対するコマンド処理を同じタイミングで制御するこ

とを特徴とする請求項1、2または3に記載の電子現金用金庫。

【請求項5】 前記通信部は、前記複数のコマンド制御部に対する診断処理を同じタイミングで制御することを特徴とする請求項1、2または3に記載の電子現金用金庫。

【請求項6】 前記通信部は、前記複数のコマンド制御部に対するコマンド処理を異なるタイミングで制御することを特徴とする請求項1、2または3に記載の電子現金用金庫。

【請求項7】 前記通信部は、前記複数のコマンド制御部に対する診断処理を異なるタイミングで制御することを特徴とする請求項1、2または3に記載の電子現金用金庫。

【請求項8】 前記インタフェース手段は、複数本のバスインタフェースより構成され、バスインタフェース毎に複数のコマンド制御部を接続させたことを特徴とする請求項3～7のいずれか一つに記載の電子現金用金庫。

【請求項9】 前記通信部は、バスインタフェース毎に接続される複数のコマンド制御部のうちで任意の転送タイミングを設定することを特徴とする請求項8に記載の電子現金用金庫。

【請求項10】 前記複数のコマンド制御部はそれぞれ異なる固有の暗号鍵を所持しており、前記通信部は、コマンド制御部別に割り当てられた前記固有の暗号鍵を所持しており、前記通信部はコマンド制御部別に割り当てられた前記固有の暗号鍵を用いて前記コマンド制御部との通信で暗号化および復号化を行い、前記コマンド制御部は自身に割り当てられた固有の暗号鍵を用いて前記通信部との通信で暗号化および復号化を行うことを特徴とする請求項1～9のいずれか一つに記載の電子現金用金庫。

【請求項11】 前記通信部は、乱数を用いて暗号鍵を生成する乱数発生器を有し、前記乱数発生器により前記各コマンド制御部に割り当てる暗号鍵を更新することを特徴とする請求項10に記載の電子現金用金庫。

【請求項12】 前記通信部と前記コマンド制御部は所定の暗号鍵を共有しており、前記通信部は、コマンド制御部側へ暗号化されたコマンドを転送する前に、当該コマンドを暗号化するために使用した暗号鍵を前記所定の暗号鍵で暗号化して通知し、前記コマンド制御部は、前記通信部により通知された暗号鍵を前記所定の暗号鍵で復号化しておき、前記復号化された暗号鍵を用いて前記通信部から転送されてくる暗号化されたコマンドを復号化することを特徴とする請求項11に記載の電子現金用金庫。

【請求項13】 通貨の価値を電子的な情報で表した電子現金を管理する上位装置と、前記上位装置の制御に従って電子現金を処理する電子現金用金庫と、

前記上位装置と前記電子現金用金庫とを接続する複数の上位バスと、  
を備え、  
前記電子現金用金庫は、  
電子現金を記憶する複数の記憶部と、  
前記複数の記憶部に対するコマンドを並列的に実行し、  
前記複数の記憶部の制御機能を実現する複数のコマンド制御部と、  
前記上位装置にそれぞれ独立した前記上位バスで接続され、前記上位装置からの要求で前記複数のコマンド制御部に対してコマンドを用いてコマンド処理を実行させる場合、もしくは、前記複数のコマンド制御部に対してコマンドを用いて診断を行う場合、前記複数のコマンド制御部との間にコマンド数に相当する通信バスを並列的に形成し、論理的に前記複数の記憶部との通信機能を実現する複数の通信部と、  
前記各コマンド制御部を前記複数の通信部に接続する複数の下位バスと、  
を有し、  
前記上位装置は、  
前記複数の上位バスのいずれか一つ以上に故障が発生した場合に他の正常な上位バスに切り換えて通信を行うことを特徴とする電子マネーシステム。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、通貨の価値を電子的な情報で表した電子現金を一括管理するための電子現金用金庫および電子マネーシステムに関し、詳細には、ICカードを用いた取引に使用される電子現金用金庫およびその電子現金用金庫を用いた電子マネーシステムに関する。

##### 【0002】

【従来の技術】近年、売買などの取引における決済の安全性と利便性の面で、従来の紙幣、貨幣などに代わる決済手段として電子的なデジタルデータを現金として利用する、いわゆる電子現金（電子マネー）が注目されている。このため、銀行などにおいて、電子現金を一括管理するための電子現金用金庫を設置する必要がある、信頼性の高い金庫の提供が求められている。

【0003】顧客がロード端末を使用してICカードに銀行側から電子現金をロードする場合、顧客のICカードと銀行側の電子現金用金庫との間で直接電子現金の交換を行う必要がある。このため、電子現金用金庫には、電子現金のデータが記憶された記憶部が設けられており、顧客のロード要求に対し顧客のICカードと電子現金用金庫の記憶部との間で直接電子現金を交換可能とする。

【0004】なお、電子現金用金庫にはセキュリティ強化が求められており、1回の電子現金移転に対する処理を多重化して、当該取引の正当性を確認する技術が提案

されている。

【0005】ここで、従来の電子現金用金庫について説明する。図24には従来の電子現金用金庫の機能的な構成が示されている。従来の電子現金用金庫は、図24に示したように、主として、通信部100にたとえば3つのコマンド制御部201、202および203を接続させた構成を備えている。コマンド制御部201、202、203は、それぞれ通信部100に対してバスインタフェース301、302、303を介して接続される。通信部100は比較器101を有しており、すべてのコマンド制御部201～203の実行結果を比較する。また、通信部100は図示せぬ上位装置にバスインタフェース400を介して上位装置から処理命令を受け付ける。

【0006】つぎに、上記電子現金用金庫の動作について説明する。図24に示した電子現金用金庫は、信頼性を向上させるため、たとえば3つのコマンド制御部201、202および203を備えている。通信部100は、上位装置からの命令に従ってコマンド制御部201～203に対して同一処理を指示し、その実行結果を受け取る。通信部100は、各コマンド制御部201～203から送られてきた実行結果を比較器101により比較し、処理の正常性を確認するなどの多重化処理を実行する。また、各コマンド制御部201～203は、電子現金としての価値を内部に保持し、通信部100からのコマンドを処理して価値を管理する。

##### 【0007】

【発明が解決しようとする課題】しかしながら、上記従来の電子現金用金庫では、通信部100の制御で各コマンド制御部201～203に対して同一処理を行うようにしているので、各コマンド制御部201～203には電子現金として同一の価値が保持されることになり、実際の価値に対して3倍の価値を物理的に保持することになった。

【0008】したがって、多重化技術を用いた不正な改造を行うとたとえば図25のようになる。図25(a)には通信部100とコマンド制御部201間のインタフェースを改造した例が示されている。図25(a)の例では、通信部100にはバスインタフェース304を介してコマンド制御部201だけを接続し、バスインタフェース304の通信部100側の3個のバスインタフェースに接続する。

【0009】また、図25(b)には通信部100とコマンド制御部202間のインタフェースを改良した例が示されている。図25(b)の例では、通信部100にはバスインタフェース305を介してコマンド制御部202だけを接続し、バスインタフェース305の通信部100側の3個のバスインタフェースに接続する。なお、図示せぬが、上記と同様に通信部100とコマンド制御部203間のインタフェースを改良した例も併せて

考えられる。

【0010】以上の如く改造された電子現金用金庫は、リバースエンジニアリングにより解析して得られるものである。このように改良すれば、通信部100には一つのコマンド制御部が接続されるだけとなる。そこで、まず図25(a)の接続すなわち通信部100とコマンド制御部201間だけの接続で価値を引き出し、その後、図25(b)の接続すなわち通信部100とコマンド制御部202間だけの接続で価値を引き出し、さらに図示せぬが通信部100とコマンド制御部203間だけの接

続で価値を引き出すと、元の価値を3倍にして現金を引き出すことができる。

【0011】上記3重化制御のように、多重化制御を利用すれば、価値を簡単に倍増して不正な多重引き出しを許してしまうという問題があった。

【0012】本発明は、上述した従来例による問題を解消するため、多重化制御による価値の多重引き出しを防止することが可能な電子現金用金庫および電子マネージシステムを提供することを目的とする。

【0013】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項1の発明に係る電子現金用金庫は、通貨の価値を電子的な情報で表した電子現金を記憶する複数の記憶部を有し、利用者とのICカードとの間で電子現金の移転を行うための電子現金用金庫であって、前記複数の記憶部に対するコマンドを並列的に実行し、前記複数の記憶部の制御機能を実現する複数のコマンド制御部と、前記複数のコマンド制御部との間にコマンド数に相当する通信バスを並列的に形成し、前記複数の記憶部との通信機能を実現する通信部と、前記複数のコマンド制御部と前記通信部とを接続し、前記通信部の制御に従って、通信部側からコマンド制御部側へ電子現金移転のためのコマンドを転送するとともにそのコマンド処理結果をコマンド制御部側から通信部側へ転送する第1インタフェース手段と、前記複数のコマンド制御部と前記通信部とを接続し、前記通信部の制御に従って、通信部側からコマンド制御部側へ診断のためのコマンドを転送するとともにその診断結果をコマンド制御部側から通信部側へ転送する第2インタフェース手段と、を備えたことを特徴とする。

【0014】この請求項1の発明によれば、第1のインタフェースで、通信部側からコマンド制御部側へ上位からのコマンドを転送するとともにそのコマンド処理結果をコマンド制御部側から通信部側へ転送し、第2のインタフェースで、通信部側からコマンド制御部側へ診断のためのコマンドを転送するとともにその診断結果をコマンド制御部側から通信部側へ転送するようにしたので、コマンド処理のバスが不正により操作されても、診断のバスから容易に不正な操作を摘発することができ、これにより、多重化制御による価値の多重引き出しを防止す

ることが可能である。

【0015】また、請求項2の発明に係る電子現金用金庫は、請求項1の発明において、前記通信部は、前記第2インタフェース手段による診断処理を前記第1インタフェース手段によるコマンド処理とは独立して制御し、前記各コマンド制御部は、前記第2インタフェース手段による診断処理を前記第1インタフェース手段によるコマンド処理とは独立して実行することを特徴とする。

【0016】この請求項2の発明によれば、コマンド処理と診断のバスがそれぞれ物理的に独立するので、バス別に不正を検出することができ、これにより、多重化制御による価値の多重引き出しを防止することが可能である。

【0017】また、請求項3の発明に係る電子現金用金庫は、通貨の価値を電子的な情報で表した電子現金を記憶する複数の記憶部を有し、利用者とのICカードとの間で電子現金の移転を行うための電子現金用金庫であって、前記複数の記憶部に対するコマンドを並列的に実行し、前記複数の記憶部の制御機能を実現する複数のコマンド制御部と、前記複数のコマンド制御部との間にコマンド数に相当する通信バスを並列的に形成し、前記複数の記憶部との通信機能を実現する通信部と、前記複数のコマンド制御部と前記通信部とを接続し、前記通信部の制御に従って、通信部側からコマンド制御部側へ電子現金移転のためのコマンドを転送するとともにそのコマンド処理結果をコマンド制御部側から通信部側へ転送することに加え、通信部側からコマンド制御部側へ診断のためのコマンドを転送するとともにその診断結果をコマンド制御部側から通信部側へ転送するインタフェース手段と、を備えたことを特徴とする。

【0018】この請求項3の発明によれば、一つのインタフェースで、通信部側からコマンド制御部側へ上位からのコマンドを転送するとともにそのコマンド処理結果をコマンド制御部側から通信部側へ転送したり、通信部側からコマンド制御部側へ診断のためのコマンドを転送するとともにその診断結果をコマンド制御部側から通信部側へ転送するようにしたので、コマンド処理のバスが不正により操作されても、データ処理上で診断のバスから容易に不正な操作を摘発することができ、これにより、多重化制御による価値の多重引き出しを防止することが可能である。

【0019】また、請求項4の発明に係る電子現金用金庫は、請求項1、2または3の発明において、前記通信部は、前記複数のコマンド制御部に対するコマンド処理を同じタイミングで制御することを特徴とする。

【0020】この請求項4の発明によれば、通信部では、複数のコマンド制御部に対するコマンド処理を同じタイミングで制御するようにしたので、不正な操作をタイミングのとり方で防止することが可能である。

【0021】また、請求項5の発明に係る電子現金用金

庫は、請求項1、2または3の発明において、前記通信部は、前記複数のコマンド制御部に対する診断処理を同じタイミングで制御することを特徴とする。

【0022】この請求項5の発明によれば、通信部では、複数のコマンド制御部に対する診断処理を同じタイミングで制御するようにしたので、不正な操作をタイミングのとり方で防止することが可能である。

【0023】また、請求項6の発明に係る電子現金用金庫は、請求項1、2または3の発明において、前記通信部は、前記複数のコマンド制御部に対するコマンド処理を異なるタイミングで制御することを特徴とする。

【0024】この請求項6の発明によれば、通信部では、複数のコマンド制御部に対するコマンド処理を異なるタイミングで制御するようにしたので、不正な操作をタイミングのとり方で防止することが可能である。

【0025】また、請求項7の発明に係る電子現金用金庫は、請求項1、2または3の発明において、前記通信部は、前記複数のコマンド制御部に対する診断処理を異なるタイミングで制御することを特徴とする。

【0026】この請求項7の発明によれば、通信部では、複数のコマンド制御部に対する診断処理を異なるタイミングで制御するようにしたので、不正な操作をタイミングのとり方で防止することが可能である。

【0027】また、請求項8の発明に係る電子現金用金庫は、請求項3～7のいずれか一つの発明において、前記インタフェース手段は、複数本のバスインタフェースより構成され、バスインタフェース毎に複数のコマンド制御部を接続させたことを特徴とする。

【0028】この請求項8の発明によれば、バスインタフェース毎に複数のコマンド制御部を接続するようにしたので、バス単位での不正防止を図ることが可能である。

【0029】また、請求項9の発明に係る電子現金用金庫は、請求項8の発明において、前記通信部は、バスインタフェース毎に接続される複数のコマンド制御部のうちで任意の転送タイミングを設定することを特徴とする。

【0030】この請求項9の発明によれば、通信部では、バスインタフェース毎に接続されるコマンド制御部内で任意の転送タイミングを設定するようにしたので、固定の順序で転送を行う場合に比べて不正防止を強化することが可能である。

【0031】また、請求項10の発明に係る電子現金用金庫は、請求項1～9のいずれか一つの発明において、前記複数のコマンド制御部はそれぞれ異なる固有の暗号鍵を所持しており、前記通信部は、コマンド制御部別に割り当てられた前記固有の暗号鍵を所持しており、前記通信部はコマンド制御部別に割り当てられた前記固有の暗号鍵を用いて前記コマンド制御部との通信で暗号化および復号化を行い、前記コマンド制御部は自身に割り当

てられた固有の暗号鍵を用いて前記通信部との通信で暗号化および復号化を行うことを特徴とする。

【0032】この請求項10の発明によれば、通信部ではコマンド制御部別に割り当てられた固有の暗号鍵を用いてコマンド制御部との通信で暗号化および復号化を行い、コマンド制御部では自身に割り当てられた固有の暗号鍵を用いて通信部との通信で暗号化および復号化を行うようにしたので、転送内容についてコマンド制御部別にセキュリティを保つことが可能である。

【0033】また、請求項11の発明に係る電子現金用金庫は、請求項10の発明において、前記通信部は、乱数を用いて暗号鍵を生成する乱数発生器を有し、前記乱数発生器により前記各コマンド制御部に割り当てる暗号鍵を更新することを特徴とする。

【0034】この請求項11の発明によれば、乱数発生器により各コマンド制御部に割り当てる暗号鍵を更新するようにしたので、暗号鍵が固定されず、これにより、不正防止を一層強化することが可能である。

【0035】また、請求項12の発明に係る電子現金用金庫は、請求項11の発明において、前記通信部と前記コマンド制御部は所定の暗号鍵を共有しており、前記通信部は、コマンド制御部側へ暗号化されたコマンドを転送する前に、当該コマンドを暗号化するために使用した暗号鍵を前記所定の暗号鍵で暗号化して通知し、前記コマンド制御部は、前記通信部により通知された暗号鍵を前記所定の暗号鍵で復号化しておき、前記復号化された暗号鍵を用いて前記通信部から転送されてくる暗号化されたコマンドを復号化することを特徴とする。

【0036】この請求項12の発明によれば、コマンド制御部側へ暗号化されたコマンドを転送する前に、当該コマンドを暗号化するために使用した暗号鍵を所定の暗号鍵で暗号化して通知し、コマンド制御部では、通信部により通知された暗号鍵を所定の暗号鍵で復号化しておき、復号化された暗号鍵を用いて通信部から転送されてくる暗号化されたコマンドを復号化するようにしたので、毎回のコマンド転送における不正防止を実現することが可能である。

【0037】また、請求項13の発明に係る電子マネーシステムは、通貨の価値を電子的な情報で表した電子現金を管理する上位装置と、前記上位装置の制御に従って電子現金を処理する電子現金用金庫と、前記上位装置と前記電子現金用金庫とを接続する複数の上位バスと、を備え、前記電子現金用金庫は、電子現金を記憶する複数の記憶部と、前記複数の記憶部に対するコマンドを並列的に実行し、前記複数の記憶部の制御機能を実現する複数のコマンド制御部と、前記上位装置にそれぞれ独立した前記上位バスで接続され、前記上位装置からの要求で前記複数のコマンド制御部に対してコマンドを用いてコマンド処理を実行させる場合、もしくは、前記複数のコマンド制御部に対してコマンドを用いて診断を行う場



合、前記複数のコマンド制御部との間にコマンド数に相当する通信バスを並列的に形成し、論理的に前記複数の記憶部との通信機能を実現する複数の通信部と、前記各コマンド制御部を前記複数の通信部に接続する複数の下位バスと、を有し、前記上位装置は、前記複数の上位バスのいずれか一つ以上に故障が発生した場合に他の正常な上位バスに切り換えて通信を行うことを特徴とする。

【0038】この請求項13の発明によれば、上位装置と電子現金用金庫内部に複数のバスを設けて、故障が発生したバスが検出されると、そのバス以外の正常なバスに切り換えて通信を行うようにしたので、通信を継続するためのフェールセーフを実現することが可能である。

【0039】

【発明の実施の形態】以下に添付図面を参照して、本発明に係る電子現金用金庫および電子マネーシステムの好適な実施の形態を詳細に説明する。

【0040】（実施の形態1）図1は本発明の電子現金用金庫が使用される電子マネーシステムを示す構成図である。図1において、銀行11には、電子現金用金庫1000、マネーサーバ1800、ホスト2000およびルータ2400が設けられている。電子現金用金庫1000は、LAN2200-1、2200-2をそれぞれ介してマネーサーバ1800に接続され、さらにホスト2000とカード管理サーバ2100がLAN2600-1および2600-2に接続される。

【0041】マネーサーバ1800は、LAN2600-1、2600-2をそれぞれ介してルータ2400に接続される。銀行1100側のルータ2400は、外部のネットワーク2800に接続され、このネットワーク2800に対してはロード端末3000が接続され、銀行1100側のマネーサーバ1800との間でユーザ3400が保有するICカード3200を使用して電子マネーの取引が可能である。ユーザ3400が保有するICカード3200を用いたロード端末3000による取引は、つぎの手順で行われる。

【0042】すなわち、

(1) ユーザ3400はICカード3200をロード端末3000にセットし、取引コードたとえば電子現金のロード、暗証番号、金額などを入力する。

(2) ロード端末3000はマネーサーバ1800を経由して電子現金用金庫1000に取引要求を行う。

(3) ロード端末3000から取引要求に対し、電子現金用金庫1000はマネーサーバ1800を介してロード端末3000にユーザ3400のICカード3200の正当性を確認するための認証要求を行う。

【0043】(4) 認証要求に対し、ロード端末3000は、ユーザ3400のICカード3200の正当性を示す認証応答を返す。

(5) 電子現金用金庫1000でロード端末3000からの認証応答を受けると、認証承認を行ってマネーサー

バ1800に伝える。

(6) マネーサーバ1800はカード管理サーバ2100に対し、ICカード3200の番号をユーザ3400が所有する預金の口座番号を変換するための口座番号などの要求を行う。

【0044】(7) カード管理サーバ2100は、マネーサーバ1800からの口座番号などの要求に対し、変換結果としての口座番号などの応答を返す。

(8) マネーサーバ1800は、ホスト2000に対し元帳更新のための取引伝聞を送信する。

(9) ホスト2000は、マネーサーバ1800からの取引電文に基づき元帳更新を行って、その結果を示す取引電文をマネーサーバ1800に応答する。

【0045】(10) マネーサーバ1800からの価値移転要求が電子現金用金庫1000に行われる。

(11) 電子現金用金庫1000のICカードとユーザ3400のICカード3200との間で価値の移転すなわち電子マネーの移転を行う。

(12) 最終的に、電子現金用金庫1000の移転終了に伴い、マネーサーバ1800からロード端末3000に取引終了に伴う取引確認を行う。

【0046】このようなICカード3200を使用した電子マネーシステムに用いる本発明の電子現金用金庫1000は、たとえばトレイ1200-1、1200-2を有し、トレイ1200-1、1200-2のそれぞれにユーザ34が保有しているICカード3200と同等な機能をソフトウェアにより論理的に実現する論理ICカード1400を、たとえば各トレイにつき32個ずつ備えている。

【0047】このように、複数のトレイ、さらには複数のICカードを設けるのは、一つの記憶部に集中して電子現金を記憶することは、セキュリティ上好ましくないこと、および複数のロード端末から同時に取引要求があった場合に、並列して処理可能にすることを鑑みてのものである。

【0048】図2は本発明の電子現金用金庫1000の外観をマネーサーバ1800とともに示している。本発明の電子現金用金庫1000は、たとえばマネーサーバ1800に併設されており、本体3500、前扉3600および後扉4000を備えている。前扉3600にはダイヤルロック3800が設けられ、所定のダイヤル番号のセットにより前扉3600を開くことができる。また、後扉4000にはシリンダ錠が取り付けられている。

【0049】図3は図2の電子現金用金庫1000の内部構造を示す断面図である。電子現金用金庫1000の本体3500は、たとえば13ミリメートルの厚さをもった鉄板で覆われており、前方に前扉3600が設けられ、後方に後扉4000が設けられている。本体3500の内部には、たとえば最大8つのトレイ1200-1

～1200-8を組み込むことができる。トレイ1200-1～1200-8に対しては、共通の回路基板となるバックパネル4200が設けられている。

【0050】バックパネル4200の背後には、トレイ1200-1～1200-8につき、それぞれ2台ずつのファンを設けたファンユニット4400が設置される。さらに本体3500の下部には、2重化された電源ユニット4600-1および4600-2と、同じく2重化されたLAN用のハブ(HUB)4800-1および4800-2が設けられている。

【0051】図4は、図3の電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表すブロック構成を示している。トレイ1200-1は、図4に示したように、通信制御部1Aと、一例であるが3重化された価値制御部とにより構成される。

【0052】3重化された価値制御部は、3つのコマンド制御部2A-1、2A-2および2A-3と、それぞれのコマンド制御部2A-1、2A-2、2A-3に接続されるICカード記憶部3A-1、3A-2、3A-3との3段により構成される。ICカード記憶部3A-1、3A-2、3A-3は、それぞれ通貨の価値を電子的な情報で表した電子現金を記憶する不揮発性メモリである。

【0053】コマンド制御部2A-1はインタフェース(図中、I/Fで示す)29-1を有し、このインタフェース29-1にICカード記憶部3A-1を接続させている。同様に、コマンド制御部2A-2、2A-3はそれぞれインタフェース(図中、I/Fで示す)29-2、29-3を有し、それぞれインタフェース29-2、29-3にICカード記憶部3A-2、3A-3を接続させている。

【0054】コマンド制御部2A-1～2A-3は、それぞれICカード記憶部3A-1～3A-3に対してコマンドを並列的に実行して論理的に複数のICカードの制御機能を実現する。これにより、電子現金のセキュリティの確保に使用している暗号処理の変更の際に、物理的な多数のICカードの交換作業を必要とすることなく、容易に変更することができる。

【0055】通信制御部1Aとコマンド制御部2A-1とは、バスインタフェース301および診断チェックバス501で接続される。同様に、通信制御部1Aとコマンド制御部2A-2とは、バスインタフェース302および診断チェックバス502で接続され、通信制御部1Aとコマンド制御部2A-3とは、バスインタフェース303および診断チェックバス503で接続される。

【0056】通信制御部1Aは、たとえば図4に示したように、LAN制御部11、MPU12A、ROM13A、RAM14、バス制御部15、比較器16、診断制御部17Aより構成される。LAN制御部11は、たと

えば100Mbit/sの100BASE-TX仕様である。このLAN制御部11は、上位インタフェースであるバスインタフェース400を介して図示せぬ上位装置すなわちマネージャサーバに接続され、TPC/IPプロトコルに従って通信を行う。MPU12Aは、LAN制御部11の制御および3重化された価値制御部の制御を行うためのプロセッサとして動作する。このMPU12AのプログラムはROM13Aに格納されており、また作業用メモリとしてRAM14が設けられている。

10 【0057】バス制御部15は、バスインタフェース301、302、303をそれぞれ経由して対応するコマンド制御部2A-1、2A-2、2A-3とのデータ転送を制御する。比較器16は、バス制御部15で転送して各コマンド制御部2A-1、2A-2、2A-3から送られてくるデータを比較する。診断制御部17Aは、診断チェックバス501～503を経由して各コマンド制御部2A-1、2A-2、2A-3へ診断コマンドを送信するとともにその診断結果を受信して3重化された価値制御部の診断を行う。

20 【0058】また、コマンド制御部2A-1は、たとえば図4に示したように、バス制御部21-1、MPU22A-1、ROM23A-1、RAM24-1、診断制御部25A-1、および、インタフェース29-1より構成される。バス制御部21-1は、バスインタフェース301を経由して対応するコマンド制御部2A-1とのデータ転送を制御する。MPU22A-1は、コマンド処理を行うためのプロセッサとして動作する。このMPU22A-1のプログラムはROM23A-1に格納されており、また作業用メモリとしてRAM24-1が設けられている。診断制御部25A-1は、診断チェックバス501を経由して通信部1Aから送られてくる診断コマンドに基づいてコマンド処理を行い、その診断結果を診断チェックバス501を経由して通信部1Aに回答する。

30 【0059】同様に、コマンド制御部2A-2は、たとえば図4に示したように、バス制御部21-2、MPU22A-2、ROM23A-2、RAM24-2、診断制御部25A-2、および、インタフェース29-2より構成される。バス制御部21-2は、バスインタフェース302を経由して対応するコマンド制御部2A-2とのデータ転送を制御する。MPU22A-2は、コマンド処理を行うためのプロセッサとして動作する。

40 【0060】このMPU22A-2のプログラムはROM23A-2に格納されており、また作業用メモリとしてRAM24-2が設けられている。診断制御部25A-2は、診断チェックバス502を経由して通信部1Aから送られてくる診断コマンドに基づいてコマンド処理を行い、その診断結果を診断チェックバス502を経由して通信部1Aに回答する。

50 【0061】同様に、コマンド制御部2A-3は、たと

例えば図4に示したように、バス制御部21-3、MPU22A-3、ROM23A-3、RAM24-3、診断制御部25A-3、および、インタフェース29-3より構成される。バス制御部21-3は、バスインタフェース303を経由して対応するコマンド制御部2A-3とのデータ転送を制御する。MPU22A-3は、コマンド処理を行うためのプロセッサとして動作する。このMPU22A-3のプログラムはROM23A-3に格納されており、また作業用メモリとしてRAM24-3が設けられている。診断制御部25A-3は、診断チェックバス503を経由して通信部1Aから送られてくる診断コマンドに基づいてコマンド処理を行い、その診断結果を診断チェックバス503を経由して通信部1Aに

【0062】つぎに動作について説明する。図5および図6は通信部側の動作を説明するフローチャートであり、図7はコマンド制御部側の動作を説明するフローチャートである。まず、通信部側の動作から説明する。図5および図6において、診断制御部17Aにより、診断チェックバス501、502、503をそれぞれ経由して対応するコマンド制御部2A-1、2A-2、2A-3へ異なる診断コマンドが送出される(ステップS101)。そして、診断制御部17Aでは、すべてのコマンド制御部2A-1~2A-3から応答信号が受信されると(ステップS102)、すべての応答すなわちすべての診断結果が比較される(ステップS103)。

【0063】その結果から、すべての診断結果が正常であるか(ステップS104、YESルート)、2つ以上の診断結果が正常、かつ、一つの診断結果が異常であるか(ステップS105、YESルート)、それとも、すべての診断結果が異常であるか(ステップS105、NOルート)の判断が下される。もしすべての診断結果が正常であれば(ステップS104、YESルート)、正常確認が行われ、上位装置に対して価値制御部の正常状態が通知される(ステップS106)。この場合、上位装置から価値制御部に対するコマンド処理のためのコマンドがバスインタフェース400を介して受信される(ステップS108)。

【0064】また、2つ以上の診断結果が正常、かつ、一つの診断結果が異常であれば(ステップS105、YESルート)、不一致すなわち異常という診断結果を得たコマンド制御部が処理対象から切り離され、そのコマンド制御部に関する異常が上位装置へ警告される(ステップS107)。この場合にも、上位装置から価値制御部に対するコマンド処理のためのコマンドがバスインタフェース400を介して受信される(ステップS108)。

【0065】また、すべての診断結果が異常であれば(ステップS105、NOルート)、すべてのコマンド制御部の動作が停止され、この異常状態が上位装置へ通

知される(ステップS109)。この場合には、通信部1Aの動作が停止される。

【0066】そして、上記ステップS108においてコマンドが受信されると、その受信コマンドは正常なコマンド制御部に対して転送され(ステップS110)、通信部1Aは応答のウェイト状態となる。今度はコマンド処理を行うことから、バスインタフェース301~303を介してコマンドが転送される。その後、応答信号すなわちコマンド処理結果がバスインタフェース301~303を介して受信されると(ステップS111)、コマンドを転送したすべての応答すなわちすべてのコマンド処理結果が比較される(ステップS112)。

【0067】その結果から、すべてのコマンド処理結果が一致であるか(ステップS113、YESルート)、2つ以上のコマンド処理結果が一致、かつ、一つのコマンド処理結果が不一致であるか(ステップS114、YESルート)、それとも、すべてのコマンド処理結果が不一致であるか(ステップS114、NOルート)の判断が下される。もしすべてのコマンド処理結果が一致であれば(ステップS113、YESルート)、正常確認が行われ(ステップS115)、上位装置に対して価値制御部の全一致状態が通知される(ステップS116)。その後、処理は継続される。

【0068】また、2つ以上のコマンド処理結果が一致、かつ、一つのコマンド処理結果が不一致であれば(ステップS114、YESルート)、不一致というコマンド処理結果を得たコマンド制御部が処理対象から切り離され(ステップS117)、そのコマンド制御部に関する不一致を含むコマンド処理結果が上位装置へ通知される(ステップS118)。この後、処理は継続される。

【0069】また、すべてのコマンド処理結果が不一致であれば(ステップS114、NOルート)、価値制御部側の異常が確認され(ステップS119)、すべてのコマンド制御部の動作が停止され、この異常状態が上位装置へ通知される(ステップS120)。この場合には、通信部1Aの動作が停止される。

【0070】以上の通信部1A側の処理に対してコマンド制御部2A-1~2A-3ではつぎのとおり処理が行われる。以下の説明で、実際には、MPUと診断制御部とは個別に処理を実行するが、一つの流れとしてここに説明する。各コマンド制御部2A-1~2A-3の処理は共通のため、代表的な処理をここに挙げる。すなわち、図7において、コマンド受信があると(ステップS201、YESルート)、その受信コマンドが診断コマンドか(ステップS202、YESルート)、それとも、上位装置からのコマンドか(ステップS205、YESルート)の判断が下される。

【0071】すなわち、バスインタフェース301~303を経由して転送されてくるコマンドは上位装置から



のコマンドとなり、診断チェックパス501~503を経由して転送されてくるコマンドは診断コマンドとなる。もし診断コマンドであれば(ステップS202、YESルート)、そのコマンドに従って診断が行われ(ステップS203)、その診断結果が通信部1Aに対して応答される(ステップS204)。そして、処理が終了でなければ(ステップS208、NOルート)、ステップS201に戻る。

【0072】また、上位装置からのコマンドであれば(ステップS205、YESルート)、その受信コマンドに従ってコマンド処理が行われ(ステップS206)、そのコマンド処理結果が通信部1Aに対して応答される(ステップS207)。一方、上位装置からのコマンドでなければ(ステップS205、NOルート)、そのコマンドに応じて処理が実行される。そして、ステップS207の後、処理が終了でなければ(ステップS208、NOルート)、ステップS201に戻る。

【0073】以上説明したように、本実施の形態1によれば、バスインタフェース301~303で、通信部側からコマンド制御部側へ上位からのコマンドを転送するとともにそのコマンド処理結果をコマンド制御部側から通信部側へ転送し、診断チェックパス501~503で、通信部側からコマンド制御部側へ診断のためのコマンドを転送するとともにその診断結果をコマンド制御部側から通信部側へ転送する。これにより、コマンド処理のバスが不正により操作されても、診断のバスから容易に不正な操作を摘発することができるので、多重化制御による価値の多重引き出しを防止することが可能である。

【0074】また、コマンド処理と診断のバスがそれぞれ物理的に独立するので、バス別に不正を検出することができる。

【0075】(実施の形態2)さて、前述した実施の形態1では、価値制御部の診断のために専用の診断チェックパスを設けていたが、本発明はこれに限定されず、以下に説明する実施の形態2のように、診断チェックパスを省いて診断処理をMPUの制御下におくようにしてもよい。この場合には、上位装置からのコマンドと診断コマンドとがマルチプレックスされることになる。なお、以下に説明する実施の形態2では、全体構成を前述した実施の形態1と同様としており、同一の構成には同一の符号を使用し、異なる構成には異なる符号を使用する。

【0076】図8は、図3の電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表す実施の形態2のブロック構成を示している。トレイ1200-1は、図8に示したように、通信制御部1Bと、一例であるが3重化された価値制御部とにより構成される。

【0077】3重化された価値制御部は、3つのコマンド制御部2B-1、2B-2および2B-3と、それぞ

れのコマンド制御部2B-1、2B-2、2B-3に接続される。ICカード記憶部3B-1、3B-2、3B-3との3段により構成される。ICカード記憶部3B-1、3B-2、3B-3は、それぞれ通貨の価値を電子的な情報で表した電子現金を記憶する不揮発性メモリである。

【0078】通信制御部1Bとコマンド制御部2B-1とは、バスインタフェース301だけで接続される。同様に、通信制御部1Bとコマンド制御部2B-2とは、バスインタフェース302だけで接続され、通信制御部1Bとコマンド制御部2B-3とは、バスインタフェース303だけで接続される。

【0079】通信制御部1Bは、たとえば図8に示したように、LAN制御部11、MPU12B、ROM13B、RAM14、バス制御部15、比較器16、診断制御部17Bより構成される。前述の実施の形態1と異なるMPU12Bは、LAN制御部11の制御、3重化された価値制御部の制御および診断制御を行うためのプロセッサとして動作する。このMPU12BのプログラムはROM13Bに格納される。なお、バス制御部15は、バスインタフェース301、302、303を介して診断コマンドおよびその診断結果を伝送し、診断制御部17Bは、MPU12Bの制御下で診断を行う。

【0080】また、コマンド制御部2B-1は、たとえば図8に示したように、バス制御部21-1、MPU22B-1、ROM23B-1、RAM24-1、診断制御部25B-1、および、インタフェース29-1より構成される。前述の実施の形態1と異なるMPU22B-1は、コマンド処理および診断制御部25B-1の制御を行うためのプロセッサとして動作する。このMPU22B-1のプログラムはROM23B-1に格納されている。診断制御部25B-1は、MPU22B-1の制御下で、バスインタフェース301を経由して通信部1Bから送られてくる診断コマンドに基づいてコマンド処理を行い、その診断結果をバスインタフェース301を経由して通信部1Bに伝答する。

【0081】同様に、コマンド制御部2B-2は、たとえば図8に示したように、バス制御部21-2、MPU22B-2、ROM23B-2、RAM24-2、診断制御部25B-2、および、インタフェース29-2より構成される。実施の形態1と異なるMPU22B-2は、コマンド処理および診断制御部25B-2の制御を行うためのプロセッサとして動作する。このMPU22B-2のプログラムはROM23B-2に格納されている。診断制御部25B-2は、MPU22B-2の制御下で、バスインタフェース302を経由して通信部1Bから送られてくる診断コマンドに基づいてコマンド処理を行い、その診断結果をバスインタフェース302を経由して通信部1Bに伝答する。

【0082】同様に、コマンド制御部2B-3は、たと

10

20

30

40

50

えば図8に示したように、バス制御部21-3、MPU22B-3、ROM23B-3、RAM24-3、診断制御部25B-3、および、インタフェース29-3より構成される。前述の実施の形態1と異なるMPU22B-3は、コマンド処理および診断制御部25B-3の制御を行うためのプロセッサとして動作する。このMPU22B-3のプログラムはROM23B-3に格納されている。診断制御部25B-3は、MPU22B-3の制御下で、バスインタフェース303を経由して通信部1Bから送られてくる診断コマンドに基づいてコマンド処理を行い、その診断結果をバスインタフェース303を経由して通信部1Bに伝送する。

【0083】 つぎに動作について説明する。図9は本実施の形態2による通信部とコマンド制御部間のタイミングチャートである。上段には、通信部1Bとコマンド制御部2B-1間のタイミングが示され、中段には、通信部1Bとコマンド制御部2B-2間のタイミングが示され、下段には、通信部1Bとコマンド制御部2B-3間のタイミングが示されている。

【0084】 通信部1Bからコマンド制御部2B-1へデータ（コマンド）が転送されると、それに対する応答（ACK）がコマンド制御部2B-1から通信部1Bに対して転送される。また、通信部1Bからコマンド制御部2B-1へ診断コマンド（診断チェック#1）が転送されると、それに対する応答（ACK）すなわち診断結果がコマンド制御部2B-1から通信部1Bに対して転送される。

【0085】 同様に、通信部1Bからコマンド制御部2B-2へデータ（コマンド）が転送されると、それに対する応答（ACK）がコマンド制御部2B-2から通信部1Bに対して転送される。また、通信部1Bからコマンド制御部2B-2へ診断コマンド（診断チェック#2）が転送されると、それに対する応答（ACK）すなわち診断結果がコマンド制御部2B-2から通信部1Bに対して転送される。

【0086】 同様に、通信部1Bからコマンド制御部2B-3へデータ（コマンド）が転送されると、それに対する応答（ACK）がコマンド制御部2B-3から通信部1Bに対して転送される。また、通信部1Bからコマンド制御部2B-3へ診断コマンド（診断チェック#3）が転送されると、それに対する応答（ACK）すなわち診断結果がコマンド制御部2B-3から通信部1Bに対して転送される。

【0087】 以上の例では、通信部1Bから各コマンド制御部2B-1～2B-3への診断コマンドの転送およびその応答受付が、同一タイミングで行われている。

【0088】 以上説明したように、本実施の形態2によれば、バスインタフェース301～303だけで、通信部側からコマンド制御部側へ上位からのコマンドを転送するとともにそのコマンド処理結果をコマンド制御部側

から通信部側へ転送したり、通信部側からコマンド制御部側へ診断のためのコマンドを転送するとともにその診断結果をコマンド制御部側から通信部側へ転送する。これにより、コマンド処理のバスが不正により操作されても、データ処理上で診断のバスから容易に不正な操作を摘発することができるので、多重化制御による価値の多重引き出しを防止することが可能である。

【0089】 また、通信部では、複数のコマンド制御部に対するコマンド処理や診断を同じタイミングで制御するようにしたので、不正な操作をタイミングのとり方で防止することが可能である。

【0090】（実施の形態3）さて、前述した実施の形態2では、同一タイミングで診断チェックを行うようにしていたが、本発明はこれに限定されず、以下に説明する実施の形態3のように、各コマンド制御部での診断タイミングをずらしてもよい。なお、以下に説明する実施の形態3では、全体構成を前述した実施の形態2と同様としており、同一の構成には同一の符号を使用し、異なる構成には異なる符号を使用する。

【0091】 ここでは、タイミングのとり方が前述の実施の形態2と相違することから、その点を説明する。図10は本実施の形態3による通信部とコマンド制御部間のタイミングチャートである。本実施の形態3では、通信部1Bに相当する通信部の符号を1C、コマンド制御部2B-1、2B-2、2B-3にそれぞれ相当するコマンド制御部の符号をそれぞれ2C-1、2C-2、2C-3として説明する。上段には、通信部1Cとコマンド制御部2C-1間のタイミングが示され、中段には、通信部1Cとコマンド制御部2C-2間のタイミングが示され、下段には、通信部1Cとコマンド制御部2C-3間のタイミングが示されている。

【0092】 通信部1Cからコマンド制御部2C-1へデータ（コマンド）が転送されると、それに対する応答（ACK）がコマンド制御部2C-1から通信部1Cに対して転送される。また、通信部1Cからコマンド制御部2C-1へ診断コマンド（診断チェック#1）が転送されると、それに対する応答（ACK）すなわち診断結果がコマンド制御部2C-1から通信部1Cに対して転送される。

【0093】 同様に、通信部1Cからコマンド制御部2C-2へデータ（コマンド）が転送されると、それに対する応答（ACK）がコマンド制御部2C-2から通信部1Cに対して転送される。また、通信部1Cからコマンド制御部2C-2へ診断コマンド（診断チェック#2）が転送されると、それに対する応答（ACK）すなわち診断結果がコマンド制御部2C-2から通信部1Cに対して転送される。

【0094】 同様に、通信部1Cからコマンド制御部2C-3へデータ（コマンド）が転送されると、それに対する応答（ACK）がコマンド制御部2C-3から通信

部1Cに対して転送される。また、通信部1Cからコマンド制御部2C-3へ診断コマンド(診断チェック#3)が転送されると、それに対する応答(ACK)すなわち診断結果がコマンド制御部2C-3から通信部1Cに対して転送される。

【0095】以上の例では、通信部1Cから各コマンド制御部2C-1~2C-3への診断コマンドの転送およびその応答受付が、異なるタイミングで行われている。

【0096】つづいて以上の異なるタイミングの発生方法について説明する。図11は本実施の形態3による通信部側の主要な動作を説明するフローチャートである。なお、コマンド制御部2C-1~2C-3に対して任意の診断順序をあらかじめ設定しておくものとする。そこで、診断順序をたとえばコマンド制御部2C-2、2C-1、2C-3として説明する。

【0097】まず、診断順位が1番のコマンド制御部から診断を行うため、その順位を示すNに“1”を設定する(ステップS301)。そして、第1番目のコマンド制御部3C-2に対して所定の診断コマンドが送出される(ステップS302)。その後、コマンド制御部3C-2から応答があると、その診断結果が受信される(ステップS303)。この段階ではすべての診断が終了していないので(ステップS304、NORルート)、Nに1が加えられ(ステップS305)、今度は第2番目のコマンド制御部3C-1に対して所定の診断コマンドが送出される(ステップS302)。

【0098】このようにしてコマンド制御部3C-1から診断結果が受信されると、同様に第3番目のコマンド制御部3C-3に対して所定の診断コマンドの転送およびその診断結果の受信が行われる。すべてのコマンド制御部への診断が終了すると(ステップS304、YESルート)、前述のステップS104へ処理が移行する。

【0099】以上説明したように、本実施の形態3によれば、通信部では、複数のコマンド制御部に対するコマンド処理を異なるタイミングで制御するようにしたので、不正な操作をタイミングのとり方で防止することが可能である。

【0100】(実施の形態4)さて、前述した実施の形態2では、各バスインタフェースに一つのコマンド制御部を接続させた構成であったが、本発明はこれに限定されず、以下に説明する実施の形態4のように、一つのバスインタフェースに複数のコマンド制御部を接続させて同一バスインタフェース上のコマンド制御部の診断を任意の順序で行うようにしてもよい。なお、以下に説明する実施の形態4では、全体構成を前述した実施の形態2と同様としており、同一の構成には同一の符号を使用し、異なる構成には異なる符号を使用する。

【0101】まず、構成について説明する。図12は、電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表す実施の形態4の

ブロック構成を示している。図12において、通信部1Dは通信部1Bと同様の構成を有しており、その内部構成についての説明は省略する。

【0102】バスインタフェース301には同一処理を行うコマンド制御部2D-11、2D-12、2D-13が接続され、バスインタフェース302には同一処理を行うコマンド制御部2D-21、2D-22、2D-23が接続され、バスインタフェース303には同一処理を行うコマンド制御部2D-31、2D-32、2D-33が接続される。コマンド制御部2D-11~2D-13、2D-21~2D-23、2D-31~2D-33は、それぞれコマンド制御部2B-1、2B-2、2B-3と同様の構成を有しており、その内部構成についての説明は省略する。

【0103】つぎに動作について説明する。図13は本実施の形態4による通信部とコマンド制御部間のタイミングチャートである。本実施の形態4では、データの説明を省略して診断動作についてのみ説明する。上段には、通信部1Dとコマンド制御部2D-11~2D-13間のタイミングが示され、中段には、通信部1Dとコマンド制御部2D-21~2D-23間のタイミングが示され、下段には、通信部1Dとコマンド制御部2D-31~2D-33間のタイミングが示されている。

【0104】本実施の形態4では、同一バスインタフェース上のコマンド制御部間には任意に診断順序が与えられる。図13において、バスインタフェース301の場合、コマンド制御部2D-11、2D-13、2D-12の順に診断が行われる。また、バスインタフェース302の場合、コマンド制御部2D-22、2D-21、2D-23の順に診断が行われ、バスインタフェース303の場合、コマンド制御部2D-33、2D-32、2D-31の順に診断が行われる。

【0105】そして、バスインタフェース間のタイミングとしては、コマンド制御部2D-11、2D-22および2D-33は同一タイミングで診断が行われ、コマンド制御部2D-13、2D-21および2D-32は同一タイミングで診断が行われ、コマンド制御部2D-12、2D-23および2D-31は同一タイミングで診断が行われる。

【0106】なお、各バスインタフェース301~303における診断順序およびバスインタフェース間での同一タイミングの組み合わせは一例であり、適宜、任意に変更可能である。

【0107】以上説明したように、本実施の形態4によれば、バスインタフェース毎に複数のコマンド制御部を接続するようにしたので、バス単位での不正防止を図ることが可能である。特に、通信部1Dでは、バスインタフェース毎に接続される複数のコマンド制御部のうちで任意の転送タイミングを設定するようにしたので、固定の順序で転送を行う場合に比べて不正防止を強化するこ

とが可能である。

【0108】（実施の形態5）さて、本発明は、以下に説明する実施の形態4のように、電子マネーの複製などを防止するため、データ転送時に暗号化処理を施すようにしてもよい。なお、以下に説明する実施の形態5では、全体構成を前述した実施の形態2と同様としており、同一の構成には同一の符号を使用し、異なる構成には異なる符号を使用する。また、本実施の形態5では、診断はしないものとする。

【0109】まず、構成について説明する。図14は、図3の電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表す実施の形態5のブロック構成を示している。トレイ1200-1は、図14に示したように、通信制御部1Eと、一例であるが3重化された価値制御部とにより構成される。

【0110】3重化された価値制御部は、3つのコマンド制御部2E-1、2E-2および2E-3と、それぞれのコマンド制御部2E-1、2E-2、2E-3に接続される。ICカード記憶部3E-1、3E-2、3E-3との3段により構成される。ICカード記憶部3E-1、3E-2、3E-3は、それぞれ通貨の価値を電子的な情報で表した電子現金を記憶する不揮発性メモリである。

【0111】通信制御部1Eとコマンド制御部2E-1とは、バスインタフェース301だけで接続される。同様に、通信制御部1Eとコマンド制御部2E-2とは、バスインタフェース302だけで接続され、通信制御部1Eとコマンド制御部2E-3とは、バスインタフェース303だけで接続される。

【0112】通信制御部1Eは、たとえば図14に示したように、LAN制御部11、MPU12E、ROM13E、RAM14、バス制御部15、比較器16、暗号化器18より構成される。前述の実施の形態1と異なるMPU12Eは、LAN制御部11の制御、3重化された価値制御部の制御および暗号化器18の制御を行うためのプロセッサとして動作する。このMPU12EのプログラムはROM13Eに格納される。暗号化器18は、コマンド制御部2E-1、2E-2、2E-3それぞれに対応させて暗号化を行うための暗号鍵a、b、cを用いてデータ（コマンド）の暗号化および復号化を行う。

【0113】また、コマンド制御部2E-1は、たとえば図14に示したように、バス制御部21-1、MPU22E-1、ROM23E-1、RAM24-1、暗号化器26-1、および、インタフェース29-1より構成される。前述の実施の形態1と異なるMPU22E-1は、コマンド処理および暗号化器26-1の制御を行うためのプロセッサとして動作する。

【0114】このMPU22E-1のプログラムはROM23E-1に格納されている。暗号化器26-1は、

MPU22E-1の制御下で、バスインタフェース301を経由して通信部1Eから送られてくるデータ（暗号化されたコマンド）に基づいて復号化処理およびコマンド処理を行い、そのコマンド処理結果を暗号化してからバスインタフェース301を経由して通信部1Eに应答する。なお、暗号化および復号化の際には、コマンド制御部2E-1対応の暗号鍵aを使用する。

【0115】同様に、コマンド制御部2E-2は、たとえば図14に示したように、バス制御部21-2、MPU22E-2、ROM23E-2、RAM24-2、暗号化器26-2、および、インタフェース29-2より構成される。実施の形態1と異なるMPU22E-2は、コマンド処理および暗号化器26-2の制御を行うためのプロセッサとして動作する。

【0116】このMPU22E-2のプログラムはROM23E-2に格納されている。暗号化器26-2は、MPU22E-2の制御下で、バスインタフェース302を経由して通信部1Eから送られてくるデータ（暗号化されたコマンド）に基づいて復号化処理およびコマンド処理を行い、そのコマンド処理結果を暗号化してからバスインタフェース302を経由して通信部1Eに应答する。なお、暗号化および復号化の際には、コマンド制御部2E-2対応の暗号鍵bを使用する。

【0117】同様に、コマンド制御部2E-3は、たとえば図14に示したように、バス制御部21-3、MPU22E-3、ROM23E-3、RAM24-3、暗号化器26-3、および、インタフェース29-3より構成される。前述の実施の形態1と異なるMPU22E-3は、コマンド処理および暗号化器26-3の制御を行うためのプロセッサとして動作する。

【0118】このMPU22E-3のプログラムはROM23E-3に格納されている。暗号化器26-3は、MPU22E-3の制御下で、バスインタフェース303を経由して通信部1Eから送られてくるデータ（暗号化されたコマンド）に基づいて復号化処理およびコマンド処理を行い、そのコマンド処理結果をバスインタフェース303を経由して通信部1Eに应答する。なお、暗号化および復号化の際には、コマンド制御部2E-3対応の暗号鍵cを使用する。

【0119】つぎにコマンド処理のタイミングについて説明する。図15は本実施の形態5による通信部とコマンド制御部間のタイミングチャートである。上段には、通信部1Eとコマンド制御部2E-1間のタイミングが示され、中段には、通信部1Eとコマンド制御部2E-2間のタイミングが示され、下段には、通信部1Eとコマンド制御部2E-3間のタイミングが示されている。

【0120】通信部1Eからコマンド制御部2E-1へデータ（暗号鍵aで暗号化されたコマンド）が転送されると、それに対する応答（ACK）がこれも暗号鍵aで暗号化されてコマンド制御部2E-1から通信部1Eに

10

20

30

40

50

対して転送される。これと同じタイミングで、通信部1 Eからコマンド制御部2 E-2ヘデータ（暗号鍵bで暗号化されたコマンド）が転送されると、それに対する応答（ACK）がこれも暗号鍵bで暗号化されてコマンド制御部2 E-2から通信部1 Eに対して転送される。同様に、通信部1 Eからコマンド制御部2 E-3ヘデータ（暗号鍵cで暗号化されたコマンド）が転送されると、それに対する応答（ACK）がこれも暗号鍵cで暗号化されてコマンド制御部2 E-3から通信部1 Eに対して転送される。

【0121】通信部1 Eとコマンド制御部2 E-1間では、コマンド#1 a、#2 a、#3 aの順にコマンド処理が実施され、通信部1 Eとコマンド制御部2 E-2間では、コマンド#1 b、#2 b、#3 bの順にコマンド処理が実施され、通信部1 Eとコマンド制御部2 E-3間では、コマンド#1 c、#2 c、#3 cの順にコマンド処理が実施される。具体的には、まずコマンド#1 a、#1 b、#1 cが同一タイミングで処理され、つぎにコマンド#2 a、#2 b、#2 cが同一タイミングで処理され、最後にコマンド#3 a、#3 b、#3 cが同一タイミングで処理される。

【0122】つぎに動作について説明する。図16は本実施の形態5による通信部側の主要な動作を説明するフローチャートであり、図17は本実施の形態5によるコマンド制御部側の動作を説明するフローチャートである。図16において、まず通信部1 Eでは、上位装置からコマンドが受信されると（ステップS401）、その受信コマンドに基づいて各コマンド制御部2 E-1、2 E-2、2 E-3へ送信すべきコマンドが生成される（ステップS402）。

【0123】その生成されたコマンドは暗号化器18により暗号鍵a、b、cを用いて暗号化され、各コマンド制御部2 E-1、2 E-2、2 E-3へ送信すべきデータ（暗号化されたコマンド）が得られる（ステップS403）。このようにして得られた3つのデータすなわち3つの暗号化されたコマンドは、バスインタフェース301、302、303を経由してそれぞれ対応するコマンド制御部2 E-1、2 E-2、2 E-3へ送信される（ステップS404）。

【0124】この後、各コマンド制御部2 E-1～2 E-3から応答信号すなわち暗号化されたコマンド処理結果が送られてくるので、受信されたコマンド処理結果に対して今度は暗号化器18において暗号鍵a、b、cを用いて復号化処理が施される（ステップS405）。このようにして各コマンド制御部2 E-1～2 E-3で処理されたコマンド処理結果が取得される。そして、処理は図6のステップS112へ移行して前述した処理を実行する。

【0125】また、各コマンド制御部2 E-1～2 E-3においては、図17の如く処理が実行される。まず、

通信部1 Eより暗号化されたコマンドが受信されると（ステップS501、YESルート）、あらかじめ用意された暗号鍵を用いてその受信されたコマンドが復号化される（ステップS502）。すなわち、コマンド制御部2 E-1においては、暗号鍵aが用意されており、暗号化器26-1はその暗号鍵aを用いて復号化を行う。同様に、コマンド制御部2 E-2においては、暗号鍵bが用意されており、暗号化器26-2はその暗号鍵bを用いて復号化を行い、コマンド制御部2 E-3においては、暗号鍵cが用意されており、暗号化器26-3はその暗号鍵cを用いて復号化を行う。

【0126】このようにして復号化が済むと、復号化されたコマンドに従ってコマンド処理が実施され（ステップS503）、そのコマンド処理結果が、コマンド制御部2 E-1であれば暗号鍵a、コマンド制御部2 E-2であれば暗号鍵b、コマンド制御部2 E-3であれば暗号鍵cを用いて暗号化される（ステップS504）。このようにして暗号化されたコマンド処理結果は通信部1 Eへ応答される（ステップS505）。

【0127】以上説明したように、本実施の形態5によれば、通信部1 Eではコマンド制御部別に割り当てられた固有の暗号鍵を用いてコマンド制御部との通信で暗号化および復号化を行い、コマンド制御部では自身に割り当てられた固有の暗号鍵を用いて通信部1 Eとの通信で暗号化および復号化を行うようにしたので、転送内容についてコマンド制御部別にセキュリティを保つことが可能である。なお、本実施の形態5においては、診断機能を除いた構成を示していたが、前述の実施の形態1～4に示した診断機能を付加してもよい。

【0128】（実施の形態6）さて、前述した実施の形態5では、各コマンド制御部に与えられる暗号鍵が固定であったが、本発明はこれに限定されず、以下に説明する実施の形態6のように、各コマンド制御部に対して暗号鍵をランダムに選定することでセキュリティを向上させるようにしてもよい。なお、以下に説明する実施の形態6では、全体構成を前述した実施の形態5と同様としており、同一の構成には同一の符号を使用し、異なる構成には異なる符号を使用する。また、本実施の形態5では、診断はしないものとする。

【0129】まず、構成について説明する。図18は、図3の電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表す実施の形態6のブロック構成を示している。トレイ1200-1は、図18に示したように、通信制御部1 Fと、一例であるが3重化された価値制御部とにより構成される。

【0130】3重化された価値制御部は、3つのコマンド制御部2 F-1、2 F-2および2 F-3と、それぞれのコマンド制御部2 F-1、2 F-2、2 F-3に接続される。ICカード記憶部3 F-1、3 F-2、3 F-3との3段により構成される。ICカード記憶部3 F



ー1, 3F-2, 3F-3は、それぞれ通貨の価値を電子的な情報で表した電子現金を記憶する不揮発性メモリである。

【0131】通信制御部1Fとコマンド制御部2F-1とは、バスインタフェース301だけで接続される。同様に、通信制御部1Fとコマンド制御部2F-2とは、バスインタフェース302だけで接続され、通信制御部1Fとコマンド制御部2F-3とは、バスインタフェース303だけで接続される。

【0132】通信制御部1Fは、たとえば図18に示したように、LAN制御部11、MPU12F、ROM13F、RAM14、バス制御部15、比較器16、暗号化器19、および、乱数発生器20より構成される。前述の実施の形態1と異なるMPU12Fは、LAN制御部11の制御、3重化された価値制御部の制御および暗号化器19の制御を行うためのプロセッサとして動作する。このMPU12FのプログラムはROM13Fに格納される。

【0133】暗号化器19は、コマンド制御部2F-1, 2F-2, 2F-3それぞれに対応させて暗号化を行うための暗号鍵c1, c2, c3や共通の暗号鍵aを用いて情報の暗号化および復号化を行う。乱数発生器20は、各コマンド制御部2F-1, 2F-2, 2F-3に与える暗号鍵をランダムに発生させる機能を有している。図18において、通信部1Fにはコマンド制御部2F-1, 2F-2, 2F-3それぞれに対応させて発生させた暗号鍵c1, c2, c3が示され、コマンド制御部2F-1, 2F-2, 2F-3には対応する暗号鍵c1, c2, c3が転送された後の状態が示されている。なお、これら暗号鍵c1, c2, c3はつぎに乱数発生器20を動作させることでたとえば暗号鍵c4, c5, c6に変化する。

【0134】また、コマンド制御部2F-1は、たとえば図18に示したように、バス制御部21-1、MPU22F-1、ROM23F-1、RAM24-1、暗号化器27-1、および、インタフェース29-1より構成される。前述の実施の形態1と異なるMPU22F-1は、コマンド処理および暗号化器27-1の制御を行うためのプロセッサとして動作する。

【0135】このMPU22F-1のプログラムはROM23F-1に格納されている。暗号化器27-1は、MPU22F-1の制御下で、バスインタフェース301を経由して通信部1Fから送られてくるデータ（暗号化されたコマンド）に基づいて復号化処理およびコマンド処理を行い、そのコマンド処理結果を暗号化してからバスインタフェース301を経由して通信部1Fに送答する。なお、暗号化および復号化の際には、コマンド制御部2F-1対応の暗号鍵c1もしくはすべてのコマンド制御部で共通の暗号鍵aを使用する。

【0136】同様に、コマンド制御部2F-2は、たと

えば図18に示したように、バス制御部21-2、MPU22F-2、ROM23F-2、RAM24-2、暗号化器27-2、および、インタフェース29-2より構成される。実施の形態1と異なるMPU22F-2は、コマンド処理および暗号化器27-2の制御を行うためのプロセッサとして動作する。

【0137】このMPU22F-2のプログラムはROM23F-2に格納されている。暗号化器27-2は、MPU22F-2の制御下で、バスインタフェース302を経由して通信部1Fから送られてくるデータ（暗号化されたコマンド）に基づいて復号化処理およびコマンド処理を行い、そのコマンド処理結果を暗号化してからバスインタフェース302を経由して通信部1Fに送答する。なお、暗号化および復号化の際には、コマンド制御部2F-2対応の暗号鍵c2もしくはすべてのコマンド制御部で共通の暗号鍵aを使用する。

【0138】同様に、コマンド制御部2F-3は、たとえば図18に示したように、バス制御部21-3、MPU22F-3、ROM23F-3、RAM24-3、暗号化器27-3、および、インタフェース29-3より構成される。前述の実施の形態1と異なるMPU22F-3は、コマンド処理および暗号化器27-3の制御を行うためのプロセッサとして動作する。

【0139】このMPU22F-3のプログラムはROM23F-3に格納されている。暗号化器27-3は、MPU22F-3の制御下で、バスインタフェース303を経由して通信部1Fから送られてくるデータ（暗号化されたコマンド）に基づいて復号化処理およびコマンド処理を行い、そのコマンド処理結果をバスインタフェース303を経由して通信部1Fに送答する。なお、暗号化および復号化の際には、コマンド制御部2F-3対応の暗号鍵c3もしくはすべてのコマンド制御部で共通の暗号鍵aを使用する。

【0140】つぎにコマンド処理のタイミングについて説明する。図19は本実施の形態6による通信部とコマンド制御部間のタイミングチャートである。上段には、通信部1Fとコマンド制御部2F-1間のタイミングが示され、中段には、通信部1Fとコマンド制御部2F-2間のタイミングが示され、下段には、通信部1Fとコマンド制御部2F-3間のタイミングが示されている。

【0141】本実施の形態6における通信部とコマンド制御部間のデータ転送では、まず通信部1Fから各コマンド制御部2F-1~2F-3へランダムに発生した暗号鍵が転送され、各コマンド制御部2F-1~2F-3で保持する暗号鍵が更新される。また、各コマンド制御部2F-1~2F-3へ転送される暗号鍵は所定の暗号鍵aにより暗号化されており、各コマンド制御部2F-1~2F-3では、あらかじめその暗号鍵aが用意されており、転送されてきた暗号鍵をその暗号鍵aで復号化する。また、コマンドに関しては、各コマンド制御部2

F-1~2F-3の暗号鍵で復号化もしくは暗号化することになる。

【0142】具体的には、まず通信部1Fからコマンド制御部2F-1へ暗号鍵aで暗号化された暗号鍵c1が転送される。同様に、通信部1Fからコマンド制御部2F-2へ暗号鍵aで暗号化された暗号鍵c2が転送され、通信部1Fからコマンド制御部2F-3へ暗号鍵aで暗号化された暗号鍵c3が転送される。

【0143】つぎのタイミングでは、通信部1Fからコマンド制御部2F-1へ暗号鍵c1で暗号化されデータ# c1が転送され、それに対する応答(ACK)がこれも暗号鍵c1で暗号化されてコマンド制御部2F-1から通信部1Fに対して転送される。これと同じタイミングで、通信部1Fからコマンド制御部2F-2へ暗号鍵c2で暗号化されたデータ# c2が転送される、それに対する応答(ACK)がこれも暗号鍵c2で暗号化されてコマンド制御部2F-2から通信部1Fに対して転送される。同様に、通信部1Fからコマンド制御部2F-3へ暗号鍵c2で暗号化されたデータ# c3が転送されると、それに対する応答(ACK)がこれも暗号鍵c3で暗号化されてコマンド制御部2F-3から通信部1Fに対して転送される。

【0144】なお、各コマンド制御部2F-1~2F-3に与えられている暗号鍵c1, c2, c3は乱数発生器20のつぎの動作によりそれぞれc4, c5, c6に変化する。したがって、図19に示したように、コマンド処理後に再度暗号鍵c4, c5, c6が通信部1F側より対応するコマンド制御部2F-1, 2F-2, 2F-3へ転送される。

【0145】つづいて通信部1Fからコマンド制御部2F-1へ暗号鍵c4で暗号化されデータ# c12が転送され、それに対する応答(ACK)がこれも暗号鍵c4で暗号化されてコマンド制御部2F-1から通信部1Fに対して転送される。これと同じタイミングで、通信部1Fからコマンド制御部2F-2へ暗号鍵c5で暗号化されたデータ# c22が転送される、それに対する応答(ACK)がこれも暗号鍵c5で暗号化されてコマンド制御部2F-2から通信部1Fに対して転送される。同様に、通信部1Fからコマンド制御部2F-3へ暗号鍵c6で暗号化されたデータ# c33が転送されると、それに対する応答(ACK)がこれも暗号鍵c6で暗号化されてコマンド制御部2F-3から通信部1Fに対して転送される。

【0146】つぎに動作について説明する。図20は本実施の形態6による通信部側の主要な動作を説明するフローチャートであり、図21は本実施の形態6によるコマンド制御部側の動作を説明するフローチャートである。図20において、まず乱数発生器20を動作させ、コマンド制御部別に固有の乱数を発生する処理が実行される。これにより得られた乱数を用いて各コマンド制

部2F-1, 2F-2, 2F-3に対応させてたとえば暗号鍵c1; c2, c3が求められる(ステップS601)。

【0147】これら暗号鍵c1, c2, c3は対応するコマンド制御部2F-1, 2F-2, 2F-3へ転送されるが、その前にあらかじめ用意された暗号鍵aにより暗号鍵c1, c2, c3自身が暗号化される(ステップS602)。そして、暗号化された暗号鍵c1, c2, c3はそれぞれ対応するコマンド制御部2F-1, 2F-2, 2F-3へ転送される。

【0148】これに対してコマンド制御部側では図21の如く処理が実行される。ここではコマンド制御部2F-1を例に挙げる。まずコマンド受信か(ステップS501、YESルート)、それとも暗号鍵の受信か(ステップS701、YESルート)の判断が下される。もしコマンド受信であれば(ステップS501、YESルート)、コマンド制御部2F-1にはすでにデータの暗号化/復号化のための暗号鍵c1が用意されていることから、その暗号鍵c1を用いて受信コマンドが復号化される(ステップS503)。

【0149】以降の説明は、すでに図13のフローで説明済みのため、省略する。一方、暗号鍵c1の受信であれば(ステップS701、YESルート)、暗号化された暗号鍵c1があらかじめ用意された暗号化aで復号化され、その復号化された暗号鍵c1が記憶される(ステップS702)。その後、処理は終了する。

【0150】以上説明したように、本実施の形態6によれば、乱数発生器20により各コマンド制御部2F-1~2F-3に割り当てる暗号鍵を更新するようにしたので、暗号鍵が固定されず、これにより、不正防止を一層強化することが可能である。なお、本実施の形態6においては、診断機能を除いた構成を示していたが、前述の実施の形態1~4に示した診断機能を付加してもよい。

【0151】また、コマンド制御部側へ暗号化されたコマンドを転送する前に、当該コマンドを暗号化するために使用した暗号鍵を所定の暗号鍵aで暗号化して通知し、コマンド制御部2F-1~2F-3では、通信部1Fにより通知された暗号鍵を所定の暗号鍵aで復号化しておき、復号化された暗号鍵を用いて通信部1Fから転送されてくる暗号化されたコマンドを復号化する。これにより、毎回のコマンド転送における不正防止を実現することが可能である。

【0152】(実施の形態7)さて、前述した実施の形態1では、1台の通信部に対して3重化された価値制御部すなわちコマンド制御部を対応させていたが、本発明はこれに限定されず、以下に説明する実施の形態7のように、複数台の通信部に対して3重化されたコマンド制御部を対応させるようにしてもよく、アクセスパスのフェールセーフを実現するようにしてもよい。なお、以下に説明する実施の形態7では、全体構成を前述した実施

の形態1と同様としており、同一の構成には同一の符号を使用し、異なる構成には異なる符号を使用する。

【0153】まず、構成について説明する。図22は、図3の電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表す実施の形態7のブロック構成を示している。トレイ1200-1は、図22に示したように、一例として2個の通信制御部1G-1、1G-2と、一例であるが3重化された価値制御部により構成される。なお、通信制御部1G-1、1G-2は、それぞれ上位装置3（マネーサーバ1800に相当する）とバスインタフェース400-1、400-2で接続される。

【0154】3重化された価値制御部は、3つのコマンド制御部2G-1、2G-2および2G-3と、それぞれのコマンド制御部2G-1、2G-2、2G-3に接続される。ICカード記憶部3G-1、3G-2、3G-3との3段により構成される。ICカード記憶部3G-1、3G-2、3G-3は、それぞれ通貨の価値を電子的な情報で表した電子現金を記憶する不揮発性メモリである。

【0155】通信制御部1G-1、1G-2とコマンド制御部2G-1とは、バスインタフェース301-1、301-2で接続される。同様に、通信制御部1G-1、1G-2とコマンド制御部2G-2とは、バスインタフェース302-1、302-2で接続され、通信制御部1G-1、1G-2とコマンド制御部2G-3とは、バスインタフェース303-1、303-2で接続される。

【0156】通信制御部1G-1は、たとえば図22に示したように、LAN制御部11-1、MPU12G-1、ROM13G-1、RAM14-1、バス制御部15-1、比較器16-1、診断制御部17G-1より構成される。なお、機能そのものについては、前述の実施の形態1と同様のため、説明を省略する。

【0157】通信制御部1G-2は、たとえば図22に示したように、LAN制御部11-2、MPU12G-2、ROM13G-2、RAM14-2、バス制御部15-2、比較器16-2、診断制御部17G-2より構成される。なお、機能そのものについては、前述の実施の形態1と同様のため、説明を省略する。

【0158】また、コマンド制御部2G-1は、たとえば図22に示したように、バス制御部28-1、MPU22G-1、ROM23G-1、RAM24-1、診断制御部25G-1、および、インタフェース29-1より構成される。バス制御部28-1は、バス制御部15-1、15-2にそれぞれバスインタフェース301-1、301-2で接続される。なお、機能そのものについては、前述の実施の形態1と同様のため、説明を省略する。

【0159】また、コマンド制御部2G-2は、たとえ

ば図22に示したように、バス制御部28-2、MPU22G-2、ROM23G-2、RAM24-2、診断制御部25G-2、および、インタフェース29-2より構成される。バス制御部28-2は、バス制御部15-1、15-2にそれぞれバスインタフェース302-1、302-2で接続される。なお、機能そのものについては、前述の実施の形態1と同様のため、説明を省略する。

【0160】また、コマンド制御部2G-3は、たとえば図22に示したように、バス制御部28-3、MPU22G-3、ROM23G-3、RAM24-3、診断制御部25G-3、および、インタフェース29-3より構成される。バス制御部28-3は、バス制御部15-1、15-2にそれぞれバスインタフェース303-1、303-2で接続される。なお、機能そのものについては、前述の実施の形態1と同様のため、説明を省略する。

【0161】ここでは、上位装置3を含む電子マネージシステムとしての動作について説明する。具体的には、各トレイの動作を管理する上位装置3の動作について説明する。図23は上位装置3によるアクセスパスの管理動作を説明するフローチャートである。上位装置3から下位側すなわちバスインタフェース400-1もしくは400-2を経由してコマンドが送信された後（ステップS801）、使用中のバスインタフェース400-1もしくは400-2に関して何等かの故障が検出された場合（ステップS802、YESルート）、正常に機能するアクセスパスすなわちもう一方の正常なバスインタフェースがあるか確認が行われる。

【0162】そして、その確認がとれると（ステップS803、YESルート）、そのもう一方のバスインタフェースを用いた通信への切り換えが行われる（ステップS804）。これにより、アクセスパスは切り換わる。そして、動作が継続される。一方、その確認がとれなければ（ステップS803、NOルート）、バスインタフェース400-1および400-2のどちらも使用不可のため、動作は停止される。なお、ステップS802において故障が検出されなければ、動作は継続される。

【0163】ここで、故障とは、バスインタフェース400-1もしくは400-2の系統で、インタフェース上、通信部上、および、コマンド制御部上のいずれかの故障を指す。

【0164】以上説明したように、本実施の形態7によれば、電子マネージシステムにおいて、上位装置3と電子現金用金庫内部に複数のパスを設けて、故障が発生したパスが検出されると、そのパス以外の正常なパスに切り換えて通信を行うようにしたので、通信を継続するためのフェールセーフを実現することが可能である。

【0165】さて、上記実施の形態7では、実施の形態1の構成を例に挙げているが、本発明はこれに限定され

ず、他の実施の形態を適用してもよい。

【0166】以上、本発明を実施の形態により説明したが、本発明の主旨の範囲内で種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【0167】

【発明の効果】以上説明したように、請求項1の発明によれば、第1のインタフェースで、通信部側からコマンド制御部側へ上位からのコマンドを転送するとともにそのコマンド処理結果をコマンド制御部側から通信部側へ転送し、第2のインタフェースで、通信部側からコマンド制御部側へ診断のためのコマンドを転送するとともにその診断結果をコマンド制御部側から通信部側へ転送するようにしたので、コマンド処理のバスが不正により操作されても、診断のバスから容易に不正な操作を摘発することができ、これにより、多重化制御による価値の多重引き出しを防止することが可能な電子現金用金庫が得られるという効果を奏する。

【0168】また、請求項2の発明によれば、請求項1の発明において、コマンド処理と診断のバスがそれぞれ物理的に独立するので、バス別に不正を検出することができ、これにより、多重化制御による価値の多重引き出しを防止することが可能な電子現金用金庫が得られるという効果を奏する。

【0169】また、請求項3の発明によれば、一つのインタフェースで、通信部側からコマンド制御部側へ上位からのコマンドを転送するとともにそのコマンド処理結果をコマンド制御部側から通信部側へ転送したり、通信部側からコマンド制御部側へ診断のためのコマンドを転送するとともにその診断結果をコマンド制御部側から通信部側へ転送するようにしたので、コマンド処理のバスが不正により操作されても、データ処理上で診断のバスから容易に不正な操作を摘発することができ、これにより、多重化制御による価値の多重引き出しを防止することが可能な電子現金用金庫が得られるという効果を奏する。

【0170】また、請求項4の発明によれば、請求項1、2または3の発明において、通信部では、複数のコマンド制御部に対するコマンド処理を同じタイミングで制御するようにしたので、不正な操作をタイミングのとり方で防止することが可能な電子現金用金庫が得られるという効果を奏する。

【0171】また、請求項5の発明によれば、請求項1、2または3の発明において、通信部では、複数のコマンド制御部に対する診断処理を同じタイミングで制御するようにしたので、不正な操作をタイミングのとり方で防止することが可能な電子現金用金庫が得られるという効果を奏する。

【0172】また、請求項6の発明によれば、請求項1、2または3の発明において、通信部では、複数のコマンド制御部に対するコマンド処理を異なるタイミング

で制御するようにしたので、不正な操作をタイミングのとり方で防止することが可能な電子現金用金庫が得られるという効果を奏する。

【0173】また、請求項7の発明によれば、請求項1、2または3の発明において、通信部では、複数のコマンド制御部に対する診断処理を異なるタイミングで制御するようにしたので、不正な操作をタイミングのとり方で防止することが可能な電子現金用金庫が得られるという効果を奏する。

【0174】また、請求項8の発明によれば、請求項3～7のいずれか一つの発明において、バスインタフェース毎に複数のコマンド制御部を接続するようにしたので、バス単位での不正防止を図ることが可能な電子現金用金庫が得られるという効果を奏する。

【0175】また、請求項9の発明によれば、請求項8の発明において、通信部では、バスインタフェース毎に接続される複数のコマンド制御部のうちで任意の転送タイミングを設定するようにしたので、固定の順序で転送を行う場合に比べて不正防止を強化することが可能な電子現金用金庫が得られるという効果を奏する。

【0176】また、請求項10の発明によれば、請求項1～9のいずれか一つの発明において、通信部ではコマンド制御部別に割り当てられた固有の暗号鍵を用いてコマンド制御部との通信で暗号化および復号化を行い、コマンド制御部では自身に割り当てられた固有の暗号鍵を用いて通信部との通信で暗号化および復号化を行うようにしたので、転送内容についてコマンド制御部別にセキュリティを保つことが可能な電子現金用金庫が得られるという効果を奏する。

【0177】また、請求項11の発明によれば、請求項10の発明において、乱数発生器により各コマンド制御部に割り当てる暗号鍵を更新するようにしたので、暗号鍵が固定されず、これにより、不正防止を一層強化することが可能な電子現金用金庫が得られるという効果を奏する。

【0178】また、請求項12の発明によれば、請求項11の発明において、コマンド制御部側へ暗号化されたコマンドを転送する前に、当該コマンドを暗号化するために使用した暗号鍵を所定の暗号鍵で暗号化して通知し、コマンド制御部では、通信部により通知された暗号鍵を所定の暗号鍵で復号化しておき、復号化された暗号鍵を用いて通信部から転送されてくる暗号化されたコマンドを復号化するようにしたので、毎回のコマンド転送における不正防止を実現することが可能な電子現金用金庫が得られるという効果を奏する。

【0179】また、請求項13の発明によれば、上位装置と電子現金用金庫内部に複数のバスを設けて、故障が発生したバスが検出されると、そのバス以外の正常なバスに切り換えて通信を行うようにしたので、通信を継続するためのフェールセーフを実現することが可能な電子

マネーシステムが得られるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の電子現金用金庫が使用される電子マネーシステムを示す構成図である。

【図2】本発明の電子現金用金庫およびマネーサーバの外観斜視図である。

【図3】図2の電子現金用金庫の内部構造を示す断面図である。

【図4】実施の形態1による電子現金用金庫の一構成例を示すブロック図である。

【図5】実施の形態1による通信部側の動作を説明するフローチャートである。

【図6】実施の形態1による通信部側の動作を説明するフローチャートである。

【図7】実施の形態1によるコマンド制御部側の動作を説明するフローチャートである。

【図8】実施の形態2による電子現金用金庫の一構成例を示すブロック図である。

【図9】実施の形態2による通信部とコマンド制御部間のタイミングチャートである。

【図10】実施の形態3による通信部とコマンド制御部間のタイミングチャートである。

【図11】実施の形態3による通信部側の主要な動作を説明するフローチャートである。

【図12】実施の形態4による電子現金用金庫の一構成例を示すブロック図である。

【図13】実施の形態4による通信部とコマンド制御部間のタイミングチャートである。

【図14】実施の形態5による電子現金用金庫の一構成例を示すブロック図である。

【図15】実施の形態5による通信部とコマンド制御部間のタイミングチャートである。

【図16】実施の形態5による通信部側の主要な動作を説明するフローチャートである。

【図17】実施の形態5によるコマンド制御部側の動作を説明するフローチャートである。

【図18】実施の形態6による電子現金用金庫の一構成例を示すブロック図である。

【図19】実施の形態6による通信部とコマンド制御部間のタイミングチャートである。

【図20】実施の形態6による通信部側の主要な動作を説明するフローチャートである。

【図21】実施の形態6によるコマンド制御部側の動作を説明するフローチャートである。

【図22】実施の形態6による電子現金用金庫を含む電子マネーシステムの主要な一構成例を示すブロック図である。

【図23】実施の形態7による動作を説明するフローチャートである。

【図24】従来の電子現金用金庫の機能的な構成を示すブロック図である。

【図25】従来の通信部とコマンド制御部間のインタフェースを改良した例を示す図である。

【符号の説明】

1A, 1B, 1D, 1E, 1F, 1G-1, 1G-2

通信部

10 2A-1~2A-3, 2B-1~2B-3 コマンド制御部

2D-11, 2D-12, 2D-13 コマンド制御部

2D-21, 2D-22, 2D-23 コマンド制御部

2D-31, 2D-32, 2D-33 コマンド制御部

2E-1~2E-3, 2F-1~2F-3 コマンド制御部

2G-1~2G-3 コマンド制御部

3 上位装置

12A, 12B, 12D, 12E, 12F, 12G-

20 1, 12G-2 MPU

13A, 13B, 13D, 13E, 13F, 13G-

1, 13G-2 ROM

16 比較器

17, 17G-1, 17G-2 診断制御部

18, 19 暗号化器

20 乱数発生器

22A-1~22A-3, 22B-1~22B-3 MPU

22E-1~22E-3 MPU

30 22F-1~22F-3, 22G-1~22G-3 MPU

23A-1~23A-3, 23B-1~23B-3 ROM

23E-1~23E-3 ROM

23F-1~23F-3, 23G-1~23G-3 ROM

25A-1~25A-3, 25B-1~25B-3 診断制御部

25G-1~25G-3 診断制御部

40 26-1~26-3, 27-1~27-3 暗号化器

301~303, 400, 400-1, 400-2 バスインタフェース

501~503 診断チェックバス

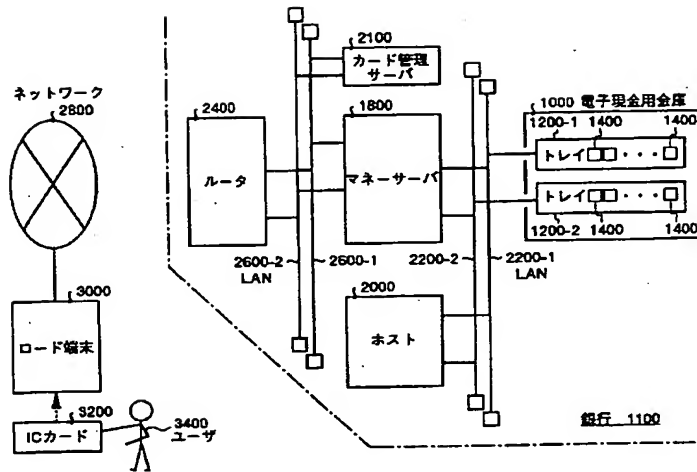
1000 金庫

1200-1, 1200-2 トレイ

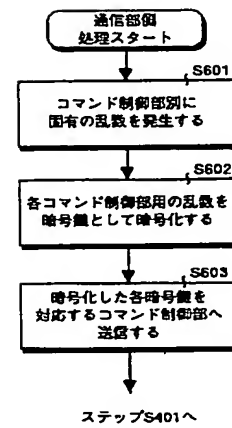
1800 マネーサーバ



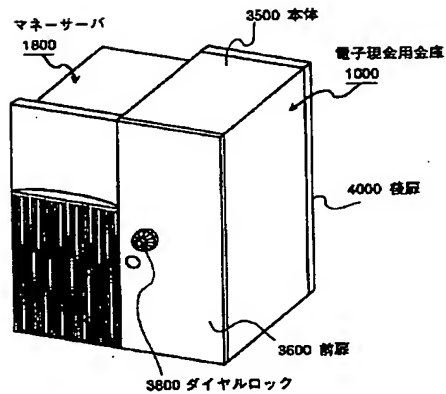
【図1】



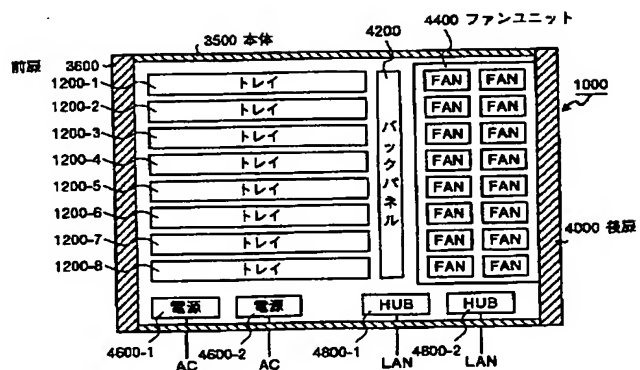
【図20】



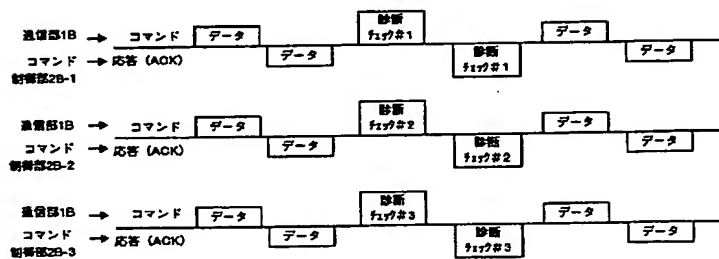
【図2】



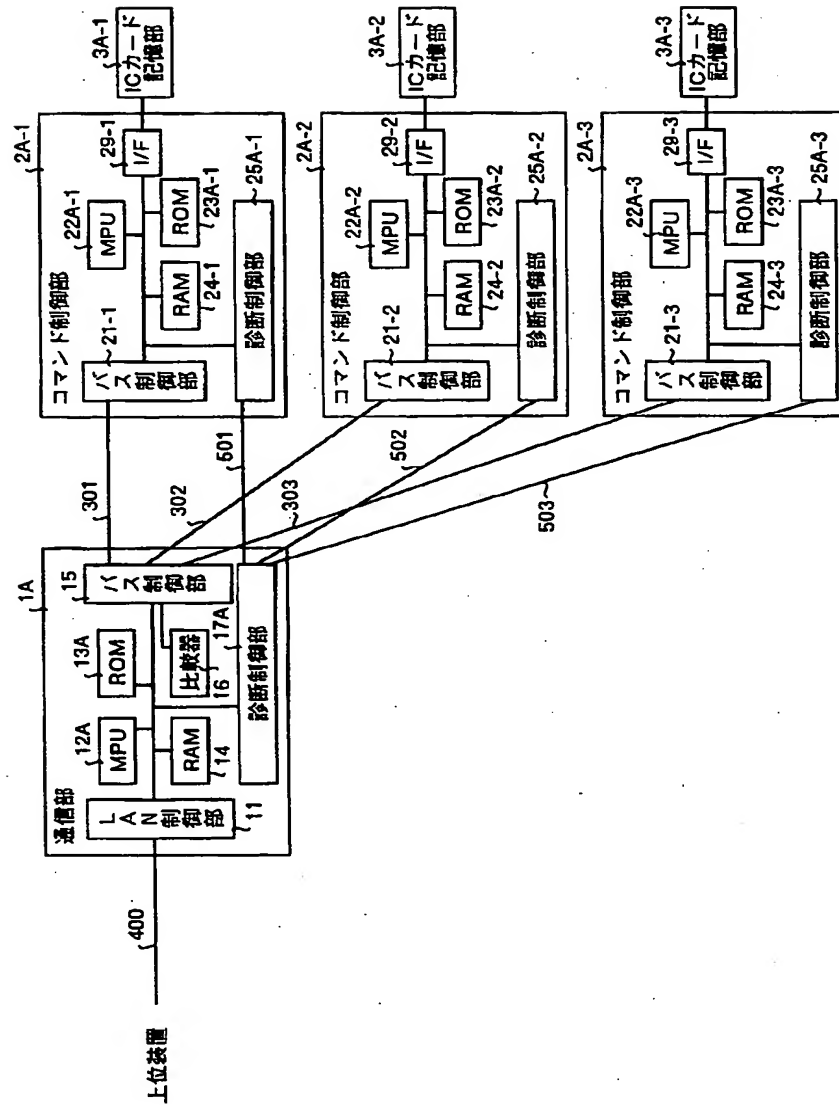
【図3】



【図9】

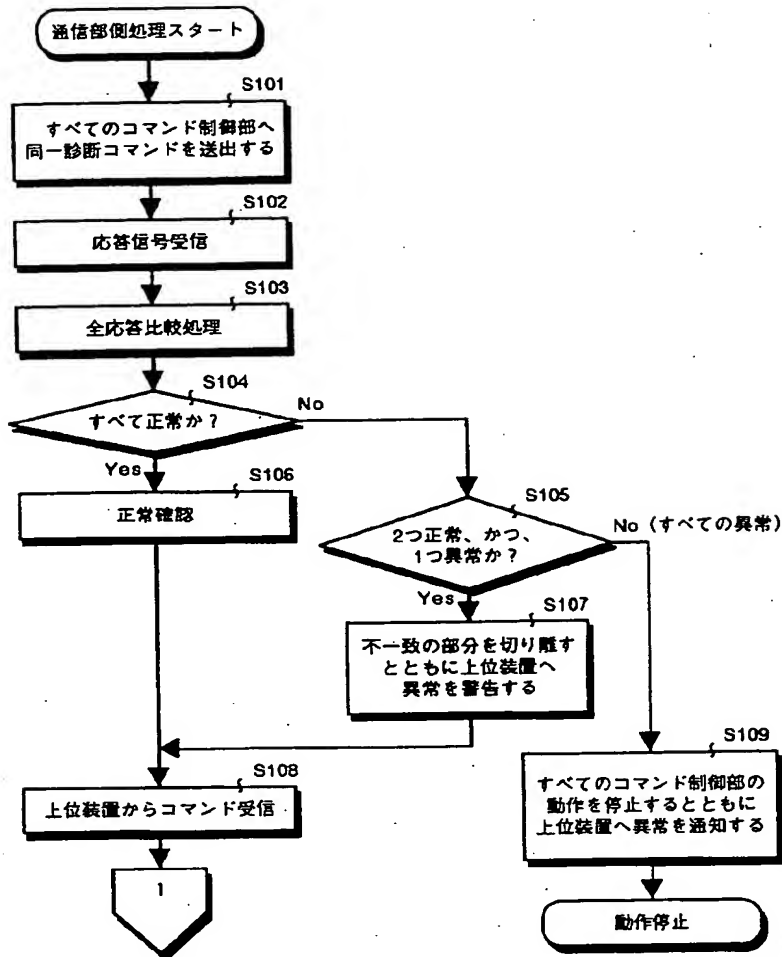


【図4】

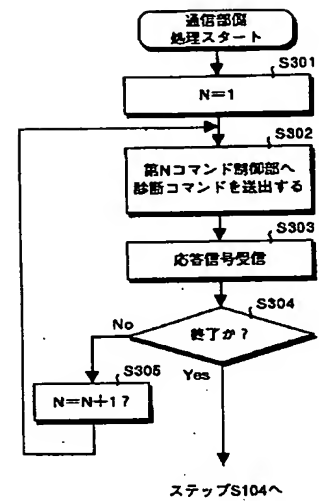


上位装置

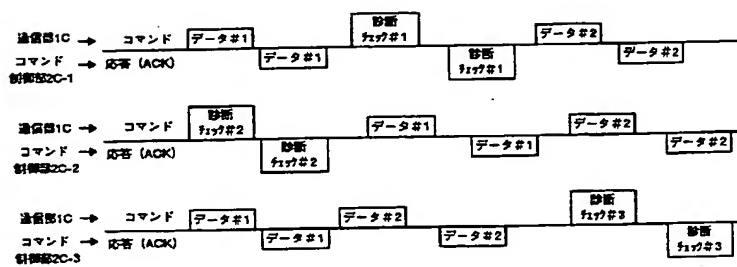
【図5】



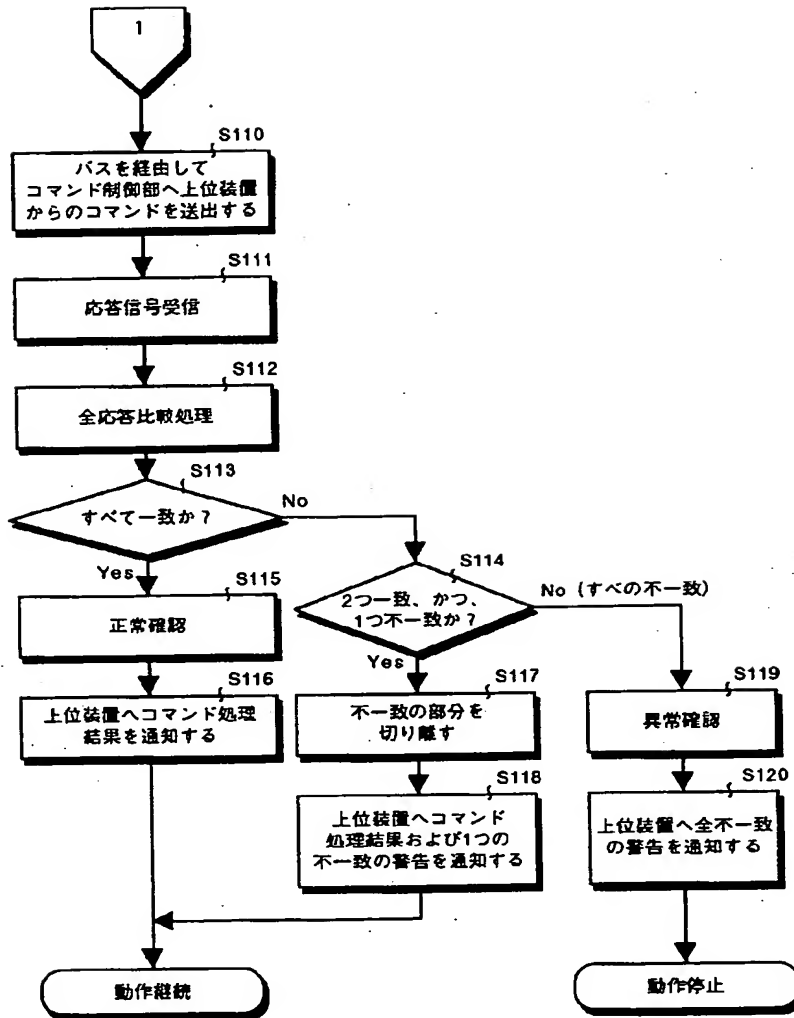
【図11】



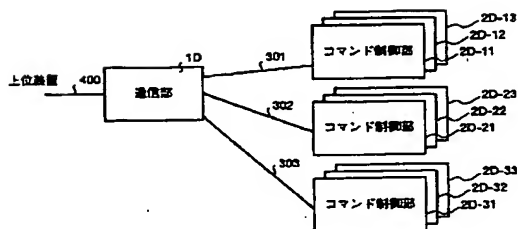
【図10】



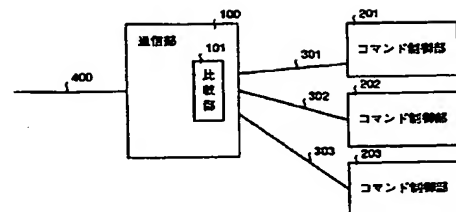
【図6】



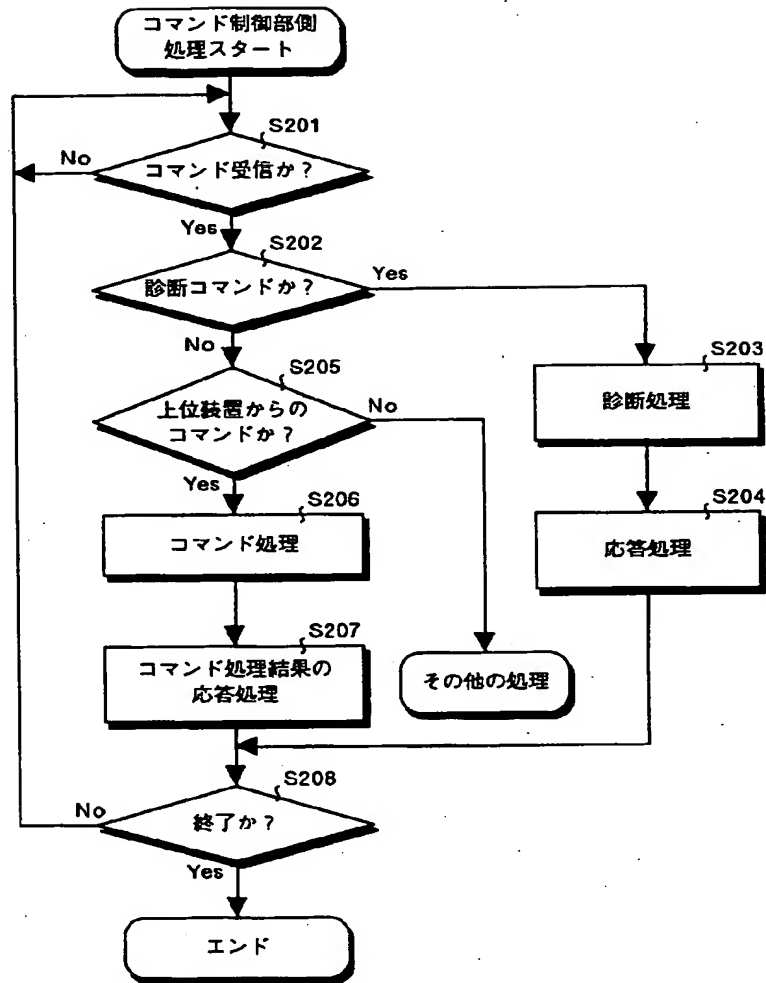
【図12】



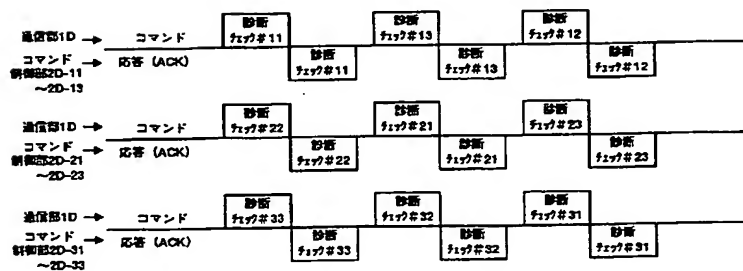
【図24】



【図7】

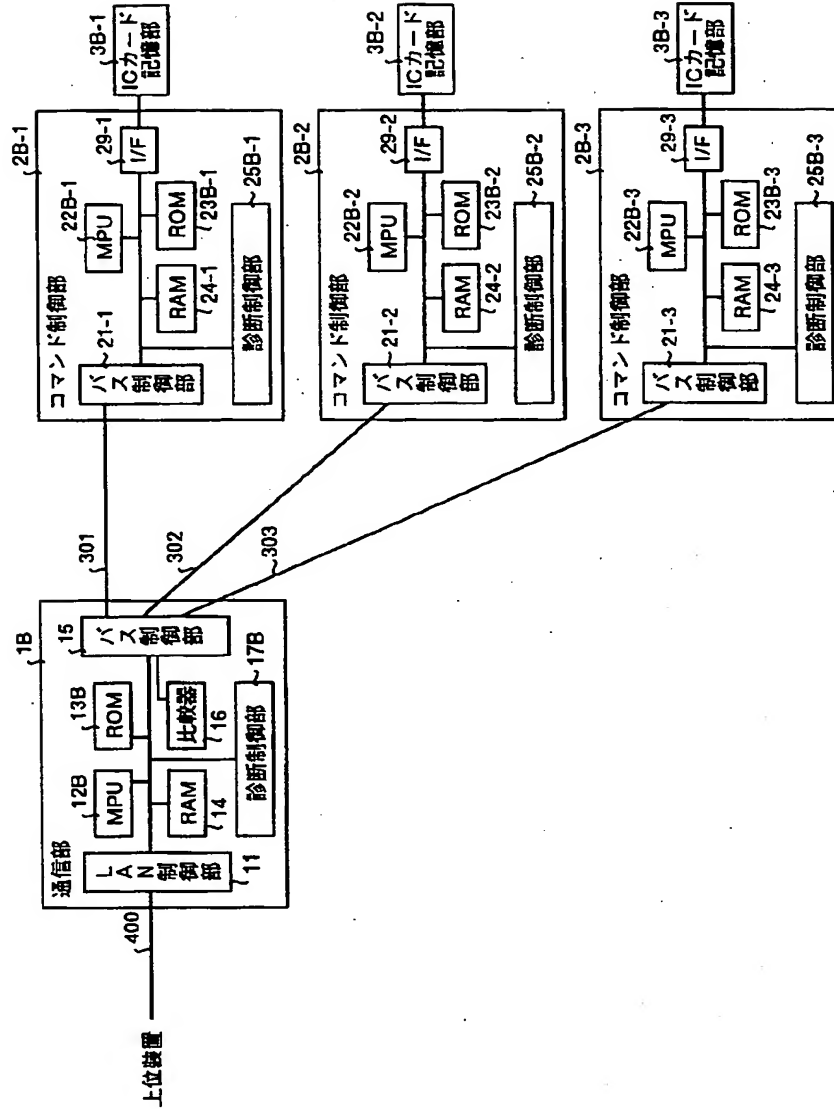


【図13】

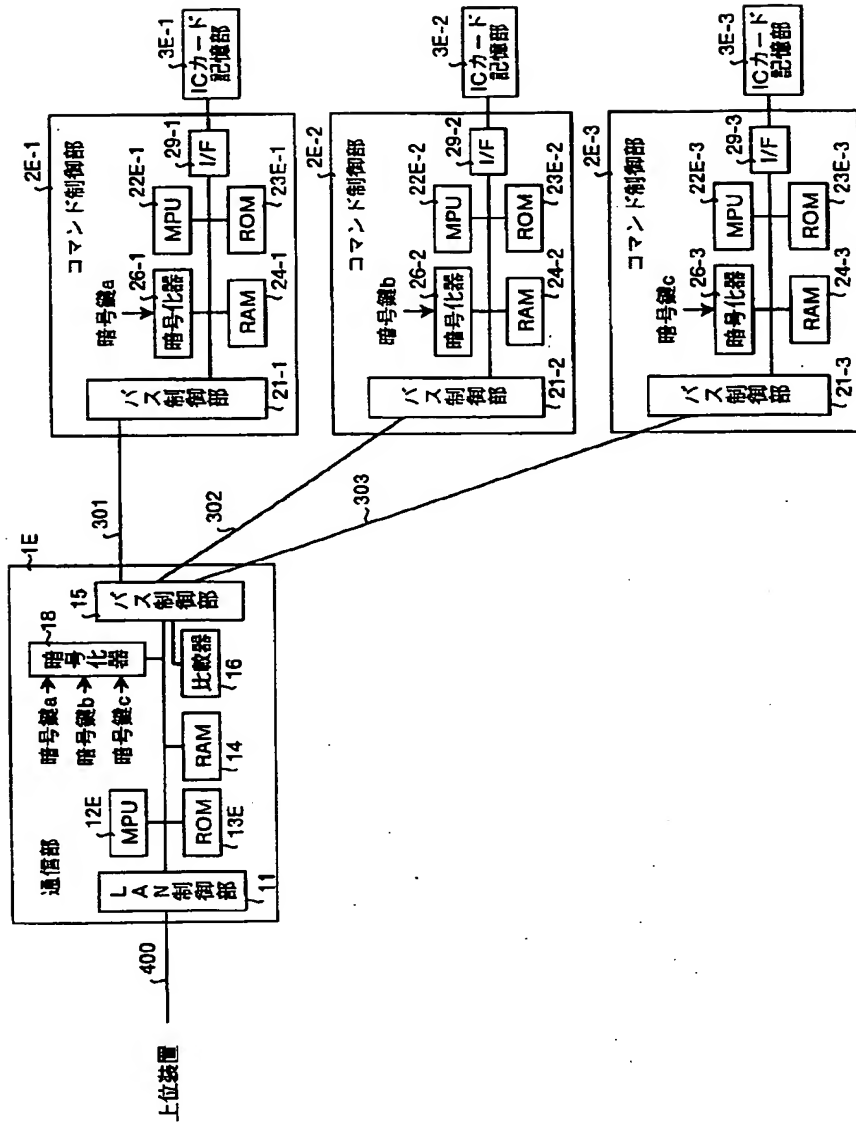




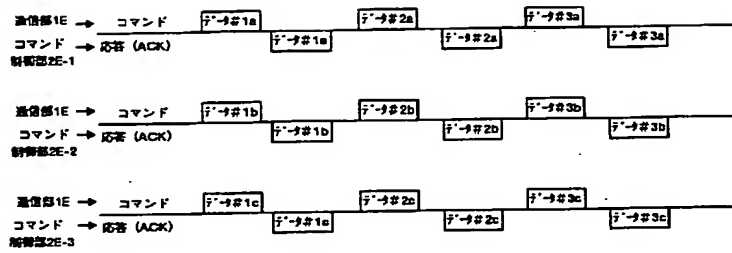
【図8】



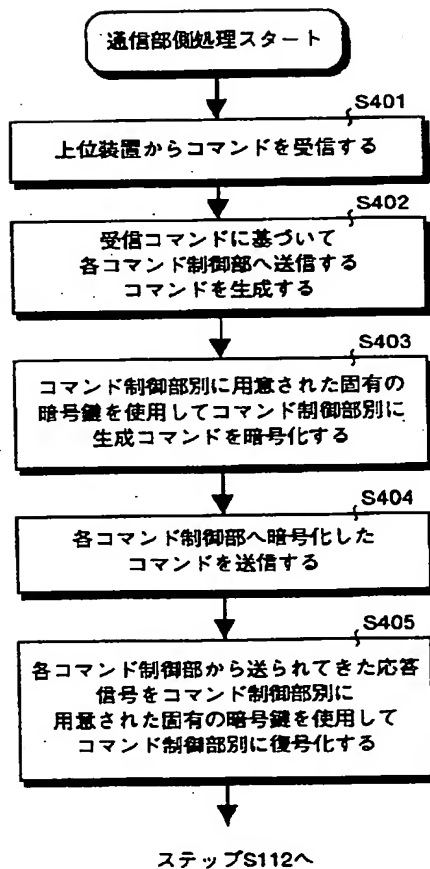
【図14】



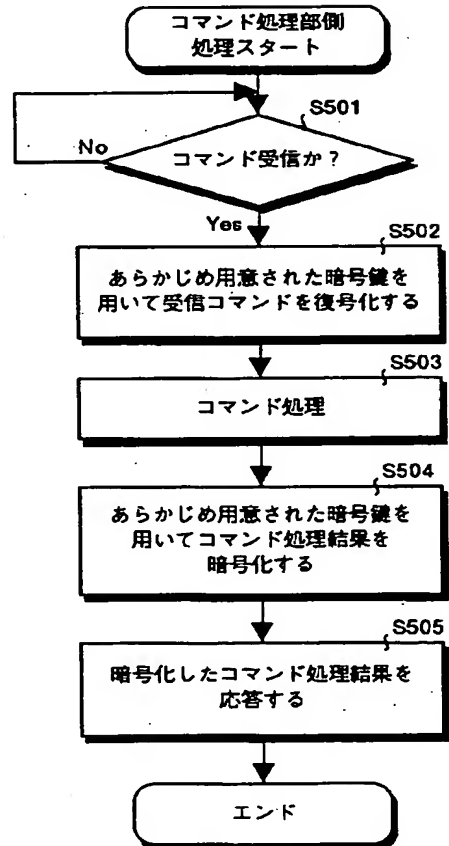
【図15】



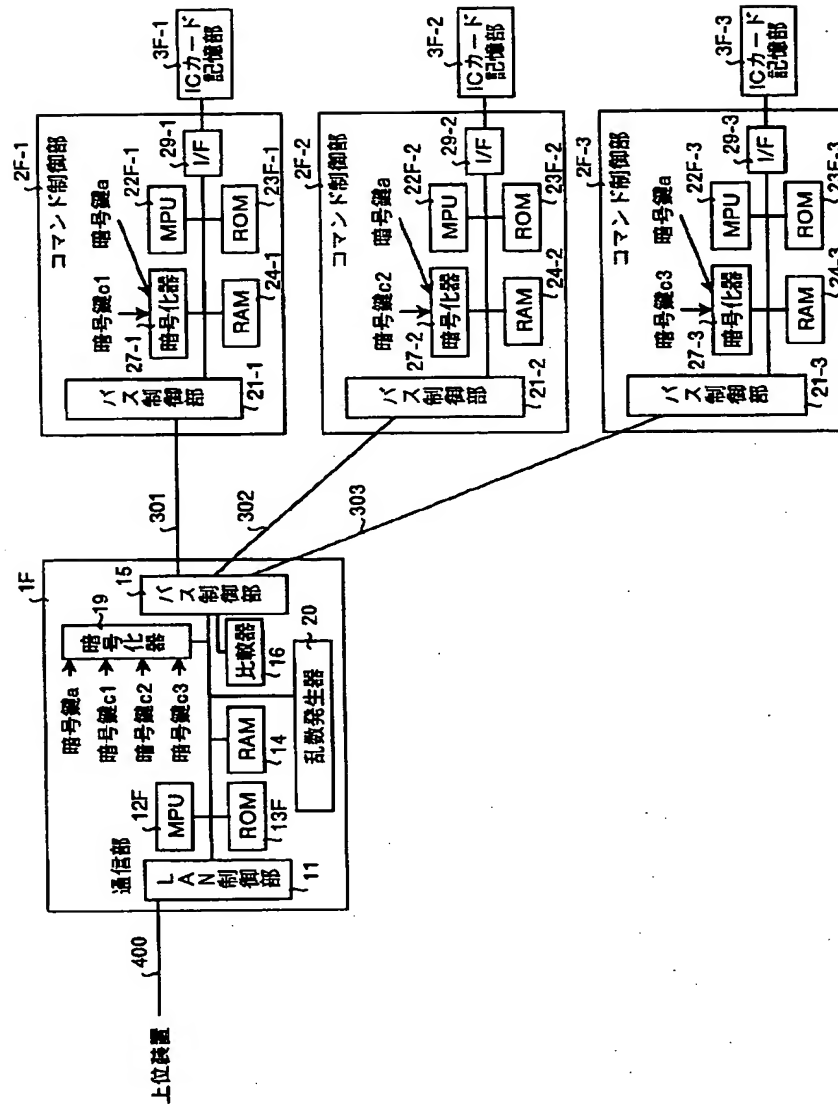
【図16】



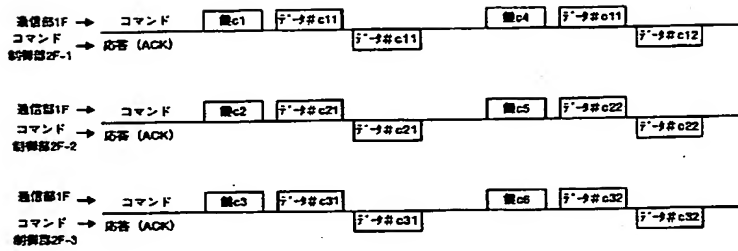
【図17】



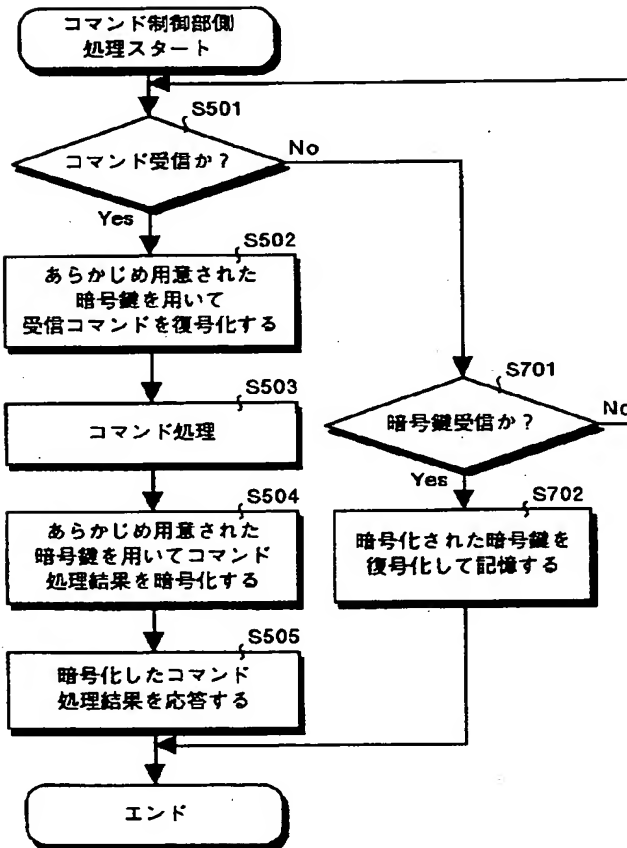
【図18】



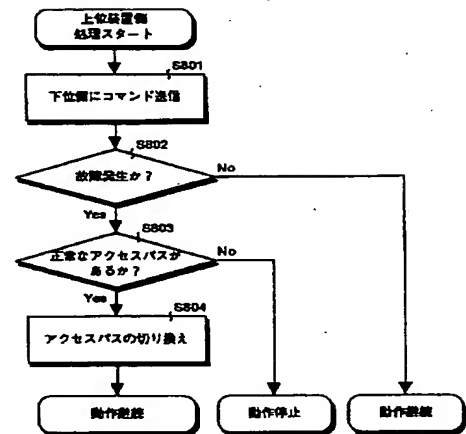
【図19】



【図21】

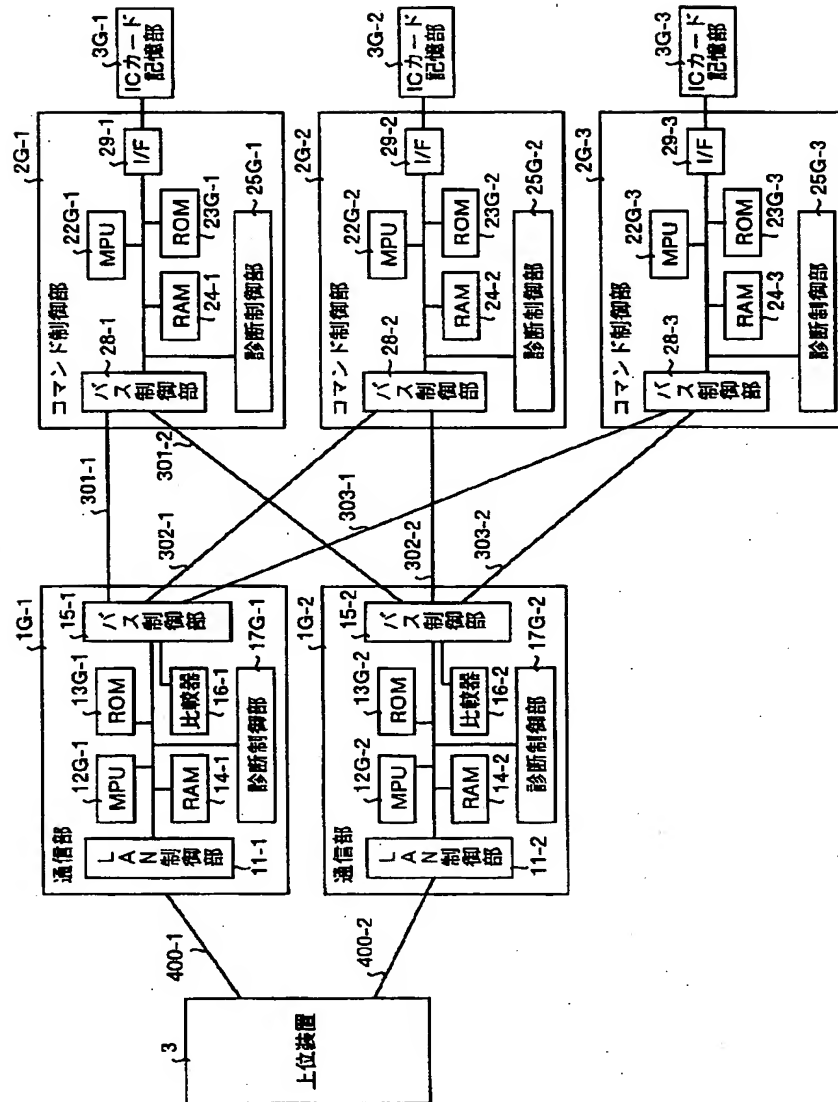


【図23】

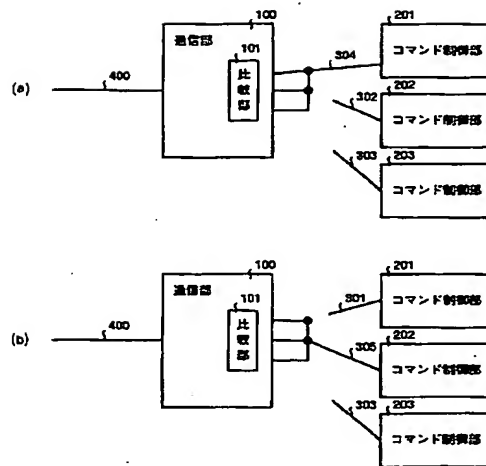




【図22】



【図 25】



## 【手続補正書】

【提出日】平成10年12月17日（1998. 12. 17）

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0040

【補正方法】変更

【補正内容】

【0040】（実施の形態1）図1は本発明の電子現金用金庫が使用される電子マネーシステムを示す構成図である。図1において、銀行1100には、電子現金用金庫1000、マネーサーバ1800、ホスト2000およびルータ2400が設けられている。電子現金用金庫1000は、LAN2200-1、2200-2をそれぞれ介してマネーサーバ1800に接続され、さらにマネーサーバ1800とカード管理サーバ2100がLAN2600-1および2600-2に接続される。

## 【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0041

【補正方法】変更

【補正内容】

【0041】マネーサーバ1800は、LAN2600-1、2600-2をそれぞれ介してルータ2400に接続される。銀行1100側のルータ2400は、外部のネットワーク2800に接続され、このネットワーク2800に対してはロード端末3000が接続され、銀行1100側のマネーサーバ1800との間でユーザ3

400が保有するICカード3200を使用して電子マネーの取引が可能である。ユーザ3400が保有するICカード3200を用いたロード端末3000による取引は、つぎの手順で行われる。

## 【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0051

【補正方法】変更

【補正内容】

【0051】図4は、図3の電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表すブロック構成を示している。トレイ1200-1は、図4に示したように、通信部1Aと、一例であるが3重化された価値制御部とにより構成される。

## 【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0055

【補正方法】変更

【補正内容】

【0055】通信部1Aとコマンド制御部2A-1とは、バスインタフェース301および診断チェックパス501で接続される。同様に、通信部1Aとコマンド制御部2A-2とは、バスインタフェース302および診断チェックパス502で接続され、通信部1Aとコマンド制御部2A-3とは、バスインタフェース303および診断チェックパス503で接続される。

## 【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0056

【補正方法】変更

【補正内容】

【0056】通信部1Aは、たとえば図4に示したように、LAN制御部11、MPU12A、ROM13A、RAM14、バス制御部15、比較器16、診断制御部17Aより構成される。LAN制御部11は、たとえば100Mbit/sの100BASE-TX仕様である。このLAN制御部11は、上位インタフェースであるバスインタフェース400を介して図示せぬ上位装置すなわちマネージャに接続され、TCP/IPプロトコルに従って通信を行う。MPU12Aは、LAN制御部11の制御および3重化された価値制御部の制御を行うためのプロセッサとして動作する。このMPU12AのプログラムはROM13Aに格納されており、また作業用メモリとしてRAM14が設けられている。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0062

【補正方法】変更

【補正内容】

【0062】つぎに動作について説明する。図5および図6は通信部側の動作を説明するフローチャートであり、図7はコマンド制御部側の動作を説明するフローチャートである。まず、通信部側の動作から説明する。図5および図6において、診断制御部17Aにより、診断チェックパス501、502、503をそれぞれ経由して対応するコマンド制御部2A-1、2A-2、2A-3へ同一の診断コマンドが送出される（ステップS101）。そして、診断制御部17Aでは、すべてのコマンド制御部2A-1～2A-3から応答信号が受信されると（ステップS102）、すべての応答すなわちすべての診断結果が比較される（ステップS103）。

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0076

【補正方法】変更

【補正内容】

【0076】図8は、図3の電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表す実施の形態2のブロック構成を示している。トレイ1200-1は、図8に示したように、通信部1Bと、一例であるが3重化された価値制御部とにより構成される。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0077

【補正方法】変更

【補正内容】

【0077】3重化された価値制御部は、3つのコマンド制御部2B-1、2B-2および2B-3と、それぞれのコマンド制御部2B-1、2B-2、2B-3に接続されるICカード記憶部3B-1、3B-2、3B-3との3段により構成される。ICカード記憶部3B-1、3B-2、3B-3は、それぞれ通貨の価値を電子的な情報で表した電子現金を記憶する不揮発性メモリである。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0078

【補正方法】変更

【補正内容】

【0078】通信部1Bとコマンド制御部2B-1とは、バスインタフェース301だけで接続される。同様に、通信部1Bとコマンド制御部2B-2とは、バスインタフェース302だけで接続され、通信部1Bとコマンド制御部2B-3とは、バスインタフェース303だけで接続される。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0079

【補正方法】変更

【補正内容】

【0079】通信部1Bは、たとえば図8に示したように、LAN制御部11、MPU12B、ROM13B、RAM14、バス制御部15、比較器16、診断制御部17Bより構成される。前述の実施の形態1と異なるMPU12Bは、LAN制御部11の制御、3重化された価値制御部の制御および診断制御を行うためのプロセッサとして動作する。このMPU12BのプログラムはROM13Bに格納される。なお、バス制御部15は、バスインタフェース301、302、303を介してコマンドおよびそのレスポンスを伝送し、診断制御部17Bは、MPU12Bの制御下で診断を行う。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0097

【補正方法】変更

【補正内容】

【0097】まず、診断順位が1番のコマンド制御部から診断を行うため、その順位を示すNに“1”を設定する（ステップS301）。そして、第1番目のコマンド制御部2C-2に対して所定の診断コマンドが送出される（ステップS302）。その後、コマンド制御部2C-2から応答があると、その診断結果が受信される（ステップS303）。この段階ではすべての診断が終了していないので（ステップS304、NORルート）、Nに1が加えられ（ステップS305）、今度は第2番目のコマンド制御部2C-1に対して所定の診断コマンドが

送出される(ステップS302)。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0098

【補正方法】変更

【補正内容】

【0098】このようにしてコマンド制御部2C-1から診断結果が受信されると、同様に第3番目のコマンド制御部2C-3に対して所定の診断コマンドの転送およびその診断結果の受信が行われる。すべてのコマンド制御部への診断が終了すると(ステップS304、YESルート)、前述のステップS103へ処理が移行する。

【手続補正13】

【補正対象書類名】明細書

【補正対象項目名】0108

【補正方法】変更

【補正内容】

【0108】(実施の形態5)さて、本発明は、以下に説明する実施の形態5のように、電子マネーの複製などを防止するため、データ転送時に暗号化処理を施すようにしてもよい。なお、以下に説明する実施の形態5では、全体構成を前述した実施の形態2と同様としており、同一の構成には同一の符号を使用し、異なる構成には異なる符号を使用する。また、本実施の形態5では、診断はしないものとする。

【手続補正14】

【補正対象書類名】明細書

【補正対象項目名】0109

【補正方法】変更

【補正内容】

【0109】まず、構成について説明する。図14は、図3の電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表す実施の形態5のブロック構成を示している。トレイ1200-1は、図14に示したように、通信部1Eと、一例であるが3重化された価値制御部とにより構成される。

【手続補正15】

【補正対象書類名】明細書

【補正対象項目名】0110

【補正方法】変更

【補正内容】

【0110】3重化された価値制御部は、3つのコマンド制御部2E-1、2E-2および2E-3と、それぞれのコマンド制御部2E-1、2E-2、2E-3に接続されるICカード記憶部3E-1、3E-2、3E-3との3段により構成される。ICカード記憶部3E-1、3E-2、3E-3は、それぞれ通貨の価値を電子的な情報で表した電子現金を記憶する不揮発性メモリである。

【手続補正16】

【補正対象書類名】明細書

【補正対象項目名】0111

【補正方法】変更

【補正内容】

【0111】通信部1Eとコマンド制御部2E-1とは、バスインタフェース301だけで接続される。同様に、通信部1Eとコマンド制御部2E-2とは、バスインタフェース302だけで接続され、通信部1Eとコマンド制御部2E-3とは、バスインタフェース303だけで接続される。

【手続補正17】

【補正対象書類名】明細書

【補正対象項目名】0112

【補正方法】変更

【補正内容】

【0112】通信部1Eは、たとえば図14に示したように、LAN制御部11、MPU12E、ROM13E、RAM14、バス制御部15、比較器16、暗号化器18より構成される。前述の実施の形態1と異なるMPU12Eは、LAN制御部11の制御、3重化された価値制御部の制御および暗号化器18の制御を行うためのプロセッサとして動作する。このMPU12EのプログラムはROM13Eに格納される。暗号化器18は、コマンド制御部2E-1、2E-2、2E-3それぞれに対応させて暗号化を行うための暗号鍵a、b、cを用いてデータ(コマンド)の暗号化および復号化を行う。

【手続補正18】

【補正対象書類名】明細書

【補正対象項目名】0118

【補正方法】変更

【補正内容】

【0118】このMPU22E-3のプログラムはROM23E-3に格納されている。暗号化器26-3は、MPU22E-3の制御下で、バスインタフェース303を経由して通信部1Eから送られてくるデータ(暗号化されたコマンド)に基づいて復号化処理およびコマンド処理を行い、そのコマンド処理結果を暗号化してからバスインタフェース303を経由して通信部1Eに応答する。なお、暗号化および復号化の際には、コマンド制御部2E-3対応の暗号鍵cを使用する。

【手続補正19】

【補正対象書類名】明細書

【補正対象項目名】0128

【補正方法】変更

【補正内容】

【0128】(実施の形態6)さて、前述した実施の形態5では、各コマンド制御部に与えられる暗号鍵が固定であったが、本発明はこれに限定されず、以下に説明する実施の形態6のように、各コマンド制御部に対して暗号鍵をランダムに選定することでセキュリティを向上さ

せるようにしてもよい。なお、以下に説明する実施の形態6では、全体構成を前述した実施の形態5と同様としており、同一の構成には同一の符号を使用し、異なる構成には異なる符号を使用する。また、本実施の形態6では、診断はしないものとする。

【手続補正20】

【補正対象書類名】明細書

【補正対象項目名】0129

【補正方法】変更

【補正内容】

【0129】まず、構成について説明する。図18は、図3の電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表す実施の形態6のブロック構成を示している。トレイ1200-1は、図18に示したように、通信部1Fと、一例であるが3重化された価値制御部とにより構成される。

【手続補正21】

【補正対象書類名】明細書

【補正対象項目名】0130

【補正方法】変更

【補正内容】

【0130】3重化された価値制御部は、3つのコマンド制御部2F-1、2F-2および2F-3と、それぞれのコマンド制御部2F-1、2F-2、2F-3に接続されるICカード記憶部3F-1、3F-2、3F-3との3段により構成される。ICカード記憶部3F-1、3F-2、3F-3は、それぞれ通貨の価値を電子的な情報で表した電子現金を記憶する不揮発性メモリである。

【手続補正22】

【補正対象書類名】明細書

【補正対象項目名】0131

【補正方法】変更

【補正内容】

【0131】通信部1Fとコマンド制御部2F-1とは、バスインタフェース301だけで接続される。同様に、通信部1Fとコマンド制御部2F-2とは、バスインタフェース302だけで接続され、通信部1Fとコマンド制御部2F-3とは、バスインタフェース303だけで接続される。

【手続補正23】

【補正対象書類名】明細書

【補正対象項目名】0132

【補正方法】変更

【補正内容】

【0132】通信部1Fは、たとえば図18に示したように、LAN制御部11、MPU12F、ROM13F、RAM14、バス制御部15、比較器16、暗号化器19、および、乱数発生器20より構成される。前述の実施の形態1と異なるMPU12Fは、LAN制御部

11の制御、3重化された価値制御部の制御および暗号化器19の制御を行うためのプロセッサとして動作する。このMPU12FのプログラムはROM13Fに格納される。

【手続補正24】

【補正対象書類名】明細書

【補正対象項目名】0139

【補正方法】変更

【補正内容】

【0139】このMPU22F-3のプログラムはROM23F-3に格納されている。暗号化器27-3は、MPU22F-3の制御下で、バスインタフェース303を経由して通信部1Fから送られてくるデータ（暗号化されたコマンド）に基づいて復号化処理およびコマンド処理を行い、そのコマンド処理結果を暗号化してからバスインタフェース303を経由して通信部1Fに回答する。なお、暗号化および復号化の際には、コマンド制御部2F-3対応の暗号鍵c3もしくはすべてのコマンド制御部で共通の暗号鍵aを使用する。

【手続補正25】

【補正対象書類名】明細書

【補正対象項目名】0143

【補正方法】変更

【補正内容】

【0143】つぎのタイミングでは、通信部1Fからコマンド制御部2F-1へ暗号鍵c1で暗号化されたデータ#c1が転送され、それに対する応答（ACK）がこれも暗号鍵c1で暗号化されてコマンド制御部2F-1から通信部1Fに対して転送される。これと同じタイミングで、通信部1Fからコマンド制御部2F-2へ暗号鍵c2で暗号化されたデータ#c2が転送される、それに対する応答（ACK）がこれも暗号鍵c2で暗号化されてコマンド制御部2F-2から通信部1Fに対して転送される。同様に、通信部1Fからコマンド制御部2F-3へ暗号鍵c3で暗号化されたデータ#c3が転送されると、それに対する応答（ACK）がこれも暗号鍵c3で暗号化されてコマンド制御部2F-3から通信部1Fに対して転送される。

【手続補正26】

【補正対象書類名】明細書

【補正対象項目名】0145

【補正方法】変更

【補正内容】

【0145】つづいて通信部1Fからコマンド制御部2F-1へ暗号鍵c4で暗号化されたデータ#c12が転送され、それに対する応答（ACK）がこれも暗号鍵c4で暗号化されてコマンド制御部2F-1から通信部1Fに対して転送される。これと同じタイミングで、通信部1Fからコマンド制御部2F-2へ暗号鍵c5で暗号化されたデータ#c22が転送される、それに対する応答

(ACK) がこれも暗号鍵 c 5 で暗号化されてコマンド制御部 2 F-2 から通信部 1 F に対して転送される。同様に、通信部 1 F からコマンド制御部 2 F-3 へ暗号鍵 c 6 で暗号化されたデータ # c 3 2 が転送されると、それに対する応答 (ACK) がこれも暗号鍵 c 6 で暗号化されてコマンド制御部 2 F-3 から通信部 1 F に対して転送される。

【手続補正 27】

【補正対象書類名】明細書

【補正対象項目名】0153

【補正方法】変更

【補正内容】

【0153】まず、構成について説明する。図22は、図3の電子現金用金庫1000に収納された8つのトレイのうち、トレイ1200-1を代表して表す実施の形態7のブロック構成を示している。トレイ1200-1は、図22に示したように、一例として2個の通信部1G-1、1G-2と、一例であるが3重化された価値制御部とにより構成される。なお、通信部1G-1、1G-2は、それぞれ上位装置3 (マネーサーバ1800に相当する) とバスインタフェース400-1、400-2で接続される。

【手続補正 28】

【補正対象書類名】明細書

【補正対象項目名】0154

【補正方法】変更

【補正内容】

【0154】3重化された価値制御部は、3つのコマンド制御部2G-1、2G-2および2G-3と、それぞれのコマンド制御部2G-1、2G-2、2G-3に接続されるICカード記憶部3G-1、3G-2、3G-3との3段により構成される。ICカード記憶部3G-1、3G-2、3G-3は、それぞれ通貨の価値を電子的な情報で表した電子現金を記憶する不揮発性メモリである。

【手続補正 29】

【補正対象書類名】明細書

【補正対象項目名】0155

【補正方法】変更

【補正内容】

【0155】通信部1G-1、1G-2とコマンド制御部2G-1とは、バスインタフェース301-1、30

1-2で接続される。同様に、通信部1G-1、1G-2とコマンド制御部2G-2とは、バスインタフェース302-1、302-2で接続され、通信部1G-1、1G-2とコマンド制御部2G-3とは、バスインタフェース303-1、303-2で接続される。

【手続補正 30】

【補正対象書類名】明細書

【補正対象項目名】0156

【補正方法】変更

【補正内容】

【0156】通信部1G-1は、たとえば図22に示したように、LAN制御部11-1、MPU12G-1、ROM13G-1、RAM14-1、バス制御部15-1、比較器16-1、診断制御部17G-1より構成される。なお、機能そのものについては、前述の実施の形態1と同様のため、説明を省略する。

【手続補正 31】

【補正対象書類名】明細書

【補正対象項目名】0157

【補正方法】変更

【補正内容】

【0157】通信部1G-2は、たとえば図22に示したように、LAN制御部11-2、MPU12G-2、ROM13G-2、RAM14-2、バス制御部15-2、比較器16-2、診断制御部17G-2より構成される。なお、機能そのものについては、前述の実施の形態1と同様のため、説明を省略する。

【手続補正 32】

【補正対象書類名】明細書

【補正対象項目名】図22

【補正方法】変更

【補正内容】

【図22】実施の形態7による電子現金用金庫を含む電子マネーシステムの主要な構成例を示すブロック図である。

【手続補正 33】

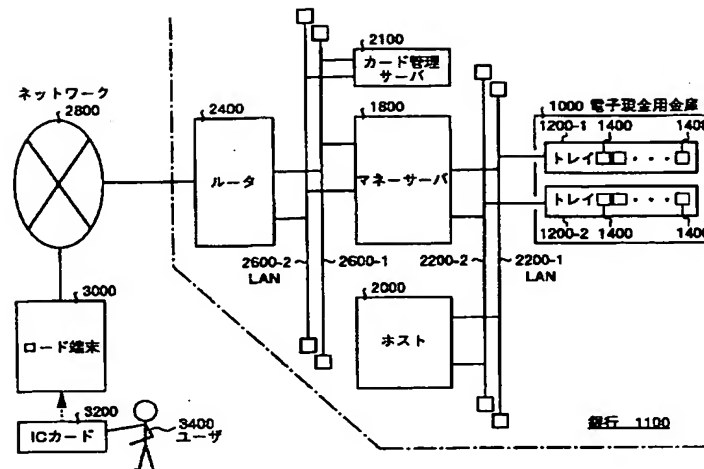
【補正対象書類名】図面

【補正対象項目名】図1

【補正方法】変更

【補正内容】

【図1】



【手続補正34】

【補正対象書類名】図面

【補正対象項目名】図11

【補正方法】変更

【補正内容】

【図11】

\* 【手続補正35】

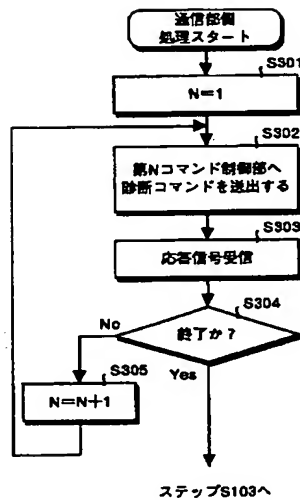
【補正対象書類名】図面

【補正対象項目名】図19

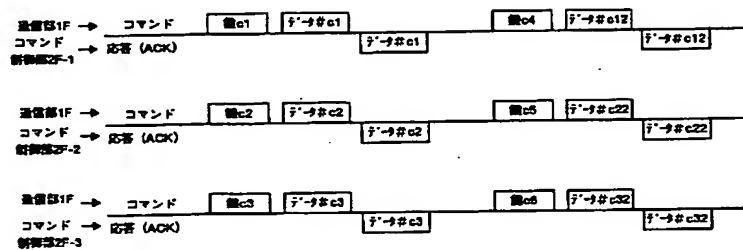
【補正方法】変更

【補正内容】

【図19】



\*



## フロントページの続き

(72)発明者 井比 俊明  
神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内  
(72)発明者 東浦 康之  
神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(72)発明者 山本 浩憲  
神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内  
Fターム(参考) 3E040 AA03 CB01 CB10 DA10 FK09  
5B055 EE01 EE15 EE17 EE27 KK05  
NC02



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**